DEFENSE OF PRIVACY ACT AND PRIVACY IN THE HANDS OF THE GOVERNMENT

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON
COMMERCIAL AND ADMINISTRATIVE LAW

AND THE

SUBCOMMITTEE ON THE CONSTITUTION

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

ON

H.R. 338

JULY 22, 2003

Serial No. 45

Printed for the use of the Committee on the Judiciary

Available via the World Wide Web: http://www.house.gov/judiciary

U.S. GOVERNMENT PRINTING OFFICE

88–543 PDF WASHINGTON : 2003

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

F. JAMES SENSENBRENNER, JR., Wisconsin, *Chairman*

HENRY J. HYDE, Illinois
HOWARD COBLE, North Carolina
LAMAR SMITH, Texas
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
STEVE CHABOT, Ohio
WILLIAM L. JENKINS, Tennessee
CHRIS CANNON, Utah
SPENCER BACHUS, Alabama
JOHN N. HOSTETTLER, Indiana
MARK GREEN, Wisconsin
RIC KELLER, Florida
MELISSA A. HART, Pennsylvania
JEFF FLAKE, Arizona
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
JOHN R. CARTER, Texas
TOM FEENEY, Florida
MARSHA BLACKBURN, Tennessee

JOHN CONYERS, JR., Michigan
HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
JERROLD NADLER, New York
ROBERT C. SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
MARTIN T. MEEHAN, Massachusetts
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida
TAMMY BALDWIN, Wisconsin
ANTHONY D. WEINER, New York
ADAM B. SCHIFF, California
LINDA T. SÁNCHEZ, California

PHILIP G. KIKO, *Chief of Staff-General Counsel*
PERRY H. APELBAUM, *Minority Chief Counsel*

SUBCOMMITTEE ON COMMERCIAL AND ADMINISTRATIVE LAW

CHRIS CANNON, Utah *Chairman*

HOWARD COBLE, North Carolina
JEFF FLAKE, Arizona
JOHN R. CARTER, Texas
MARSHA BLACKBURN, Tennessee
STEVE CHABOT, Ohio
TOM FEENEY, Florida

MELVIN L. WATT, North Carolina
JERROLD NADLER, New York
TAMMY BALDWIN, Wisconsin
WILLIAM D. DELAHUNT, Massachusetts
ANTHONY D. WEINER, New York

RAYMOND V. SMIETANKA, *Chief Counsel*
SUSAN A. JENSEN, *Counsel*
DIANE K. TAYLOR, *Counsel*
JAMES DALEY, *Full Committee Counsel*
STEPHANIE MOORE, *Minority Counsel*

SUBCOMMITTEE ON THE CONSTITUTION

STEVE CHABOT, Ohio, *Chairman*

STEVE KING, Iowa
WILLIAM L. JENKINS, Tennessee
SPENCER BACHUS, Alabama
JOHN N. HOSTETTLER, Indiana
MELISSA A. HART, Pennsylvania
TOM FEENEY, Florida
J. RANDY FORBES, Virginia

JERROLD NADLER, New York
JOHN CONYERS, JR., Michigan
ROBERT C. SCOTT, Virginia
MELVIN L. WATT, North Carolina
ADAM B. SCHIFF, California

CRYSTAL M. ROBERTS, *Chief Counsel*
PAUL B. TAYLOR, *Counsel*
D. MICHAEL HURST, JR., *Counsel*
DAVID LACHMANN, *Minority Professional Staff Member*

CONTENTS

JULY 22, 2003

OPENING STATEMENT

WITNESSES

LETTERS, STATEMENTS, ETC., SUBMITTED FOR THE HEARING

DEFENSE OF PRIVACY ACT AND PRIVACY IN THE HANDS OF THE GOVERNMENT

TUESDAY, JULY 22, 2003

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COMMERCIAL
AND ADMINISTRATIVE LAW,

AND

SUBCOMMITTEE ON THE CONSTITUTION,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittees met, pursuant to call, at 10:10 a.m., in Room 2141, Rayburn House Office Building, Hon. Chris Cannon [Chairman of the Subcommittee on Commercial and Administrative Law] presiding.

Mr. CANNON. We are waiting because we would like to introduce Ms. Murphy appropriately, and we are waiting for a faxed resume to come in. But while we're waiting, if you wouldn't mind, Steve, I thought we could swear the witnesses. So if Mr. Barr, Mr. Dempsey and Ms. Murphy, if you would stand and raise your right hand and take an oath, I would appreciate that.

[Witnesses sworn.]

Mr. CANNON. The record should reflect that everyone said yes. And we will wait just, if you don't mind, another moment or two before we get started.

[Recess.]

Mr. CANNON. The Subcommittees will come to order. On behalf of the Commercial and Administrative Law Subcommittee, I want to express our sincere appreciation to our colleague and friend, the esteemed Chair of the Constitution Subcommittee, and its Members for participating today with us in this joint hearing on H.R. 338, the "Defense of Privacy Act."

The fact that this is a joint hearing underscores the broad-ranging ramifications of the subject matter.

The Government's collection, use, dissemination and protection of personally identifiable information presents far-reaching regulatory as well as constitutional issues, especially in these days when there is an increasingly critical need to balance law enforcement initiatives designed to preemptively detect and deter terrorist attacks and other crimes, with the need to protect the privacy of innocent Americans from abusive and potentially destructive Government intrusion. H.R. 338, I believe, strikes that important balance, and I thank my co-chair for taking the initiative to reintroduce this bill in the 108th Congress.

H.R. 338 imposes a modest, though meaningful, requirement that a Federal agency prepare a privacy impact analysis for proposed and final rules noticed for public comment. H.R. 338 is intended to ensure that individual privacy rights are safeguarded by requiring Federal agencies to consider the privacy implications presented by the collection, use, and dissemination of personally identifiable information.

On the other hand, H.R. 338 will not overly burden the work of these agencies. In fact, its analysis requirement is similar to other analyses that agencies currently conduct, such as those required by the Regulatory Flexibility Act and the E-Government Act of 2002. And the Congressional Budget Office has concluded with respect to H.R. 338's identical predecessor in the 107th Congress that implementation of this measure would not entail significant costs.

As technological developments increasingly facilitate the collection and dissemination of personally identifiable information, the potential for misuse of such information grows. The General Accounting Office has warned that our Nation's increasing ability to accumulate, store, retrieve, cross-reference, analyze and link vast numbers of electronic records brings substantial Federal information benefits as well as increasing responsibilities and concerns.

The misuse—and I suspect some of the Members of the panel will think that was an understatement, and that's what we're actually looking to explore—the misuse of personally identifiable information by the Federal Government presents two major concerns. One is the potential for fraud presented by unrestricted access to such information by unscrupulous individuals, such as identity thieves. According to the Federal Trade Commission, identify theft has become one of the most widely reported consumer crimes in recent years. In fact, the Identity Theft Resource Center reports an estimated 700,000 Americans have been victims of this devastating form of fraud.

The other concern relates to the privacy ramifications and to issues presented when the Government relies on inaccurate personally identifiable information. This concern is perhaps best illustrated by certain data-mining activities being undertaken by various Federal agencies. Data mining apparently involves a complex system that utilizes sophisticated data analysis tools to scan large databases for purposes of identifying valid patterns and relationships. For example, data mining is currently being used by the Justice Department to assess crime patterns and adjust resource allotments, and by the Veterans Administration to predict demographic changes for budgetary purposes. The Defense Department as well as the Transportation Security Administration are also exploring data mining's terrorism-detection capabilities.

Nevertheless, privacy advocates as well as the Congressional Research Service have identified certain concerns relating to the accuracy and privacy implications of data mining. The Congressional Research Service, for instance, noted that if a database contains inaccurate information, innocent people could be branded security risks on the basis of flawed data and without any meaningful way to challenge the Government's determination. In addition, House Judiciary Committee Chairman Jim Sensenbrenner has also warned that the Defense Department's Terrorism Information

Awareness Data Mining Project warrants careful scrutiny because of its implications to civil liberties, mainly the presumption of innocence and the right to be free from intrusive Government surveillance absent particularized suspicion of criminal wrongdoing.

At least in response to the regulatory aspects of privacy in the hands of the Government, H.R. 338 offers a simple noncontroversial solution that requires Federal agencies to consider the privacy ramifications with respect to proposed and final rules. As some of you may recall, bipartisan legislation similar to H.R. 338 was introduced by Mr. Chabot in the 106th Congress, and a bill virtually identical to H.R. 338 was introduced by Mr. Barr in the 107th Congress. In the last Congress the Commercial and Administrative Law Subcommittee, of which Mr. Barr was Chairman, held a hearing on this measure's predecessor at which a broad political spectrum of witnesses testified in support of the legislation. The bill was ordered favorably reported by our Subcommittee as well as by the full Committee without amendment by voice vote. Thereafter, the House under suspension of rules passed the bill without amendment by voice vote in October of last year. Unfortunately the Senate did not consider the bill prior to the conclusion of the 107th Congress.

It is against this substantial background that we will consider H.R. 338.

[The prepared statement of Mr. Cannon follows:]

PREPARED STATEMENT OF THE HONORABLE CHRIS CANNON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF UTAH

On behalf of the Commercial and Administrative Law Subcommittee, I want to express our sincere appreciation to our colleague and friend, the esteemed Chair of the Constitution Subcommittee and its Members for participating today with us in this joint hearing on H.R. 338, the "Defense of Privacy Act."

The very fact that this is a joint hearing underscores the broad-ranging ramifications of the subject matter. The government's collection, use, dissemination, and protection of personally identifiable information presents far-reaching regulatory as well as constitutional issues. Especially in these days, there is an increasingly critical need to balance law enforcement initiatives designed to preemptively detect and deter terrorist attacks and other crimes with the need to protect the privacy of innocent Americans from obtrusive and potentially destructive governmental intrusions.

H.R. 338, I believe, strikes that important balance and I thank my Co-Chair for taking the initiative to re-introduce this bill in the 108th Congress. H.R. 338 imposes a modest, though meaningful, requirement that a federal agency prepare a privacy impact analysis for proposed and final rules noticed for public comment. H.R. 338 is intended to ensure that individual privacy rights are safeguarded by requiring federal agencies to consider the privacy implications presented by the collection, use, and dissemination of personally identifiable information.

On the other hand, H.R. 338 will not overly burden the work of these agencies. In fact, its analysis requirement is similar to other analyses that agencies currently conduct, such as those required by the Regulatory Flexibility Act and the E-Government Act of 2002. And, the Congressional Budget Office has concluded—with respect to H.R. 338's identical predecessor in the 107th Congress—that implementation of this measure would not entail "significant costs."

As technological developments increasingly facilitate the collection and dissemination of personally identifiable information, the potential for misuse of such information grows. The General Accounting Office has warned that our nation's "increasing ability to accumulate, store, retrieve, cross-reference, analyze, and link vast numbers of electronic records" brings "substantial federal information benefits as well as increasing responsibilities and concerns."

The misuse of personally identifiable information by the federal government presents two major concerns. One is the potential for fraud presented by unrestricted access to such information by unscrupulous individuals such as identity thieves. According to the Federal Trade Commission, identity theft has become one of the most

widely reported consumer crimes in recent years. In fact, the Identity Theft Resource Center reports that an estimated 700,000 Americans have been victims of this devastating form of fraud.

The other concern relates to the privacy ramifications and to issues presented when the government relies on inaccurate personally identifiable information. This concern is perhaps best illustrated by certain data mining activities being undertaken by various federal agencies. Data mining apparently involves a complex system that utilizes sophisticated data analysis tools to scan large databases for the purpose of identifying "valid patterns and relationships." For example, data mining is currently being used by the Justice Department to assess crime patterns and adjust resource allotments and by the Veterans Administration to predict demographic changes for budgetary purposes. The Defense Department as well as the Transportation Security Administration are also exploring data mining's terrorism detection capabilities.

Nevertheless, privacy advocates as well as the Congressional Research Service have identified certain concerns relating to the accuracy and privacy implications of data mining. The Congressional Research Service, for instance, noted that if a database contains inaccurate information, "innocent people could be branded security risks on the basis of flawed data and without any meaningful way to challenge the government's determination." In addition, House Judiciary Committee Chairman Jim Sensenbrenner has also warned that the Defense Department's Terrorism Information Awareness data mining project "warrants careful scrutiny because of its implications to civil liberties, mainly the presumption of innocence and the right to be free from intrusive government surveillance absent particularized suspicion of criminal wrongdoing."

At least in response to the regulatory aspects of privacy in the hands of the government, H.R. 338 offers a simple, noncontroversial solution that requires federal agencies to consider the privacy ramifications with respect to proposed and final rules. As some of you may recall, bipartisan legislation similar to H.R. 338 was introduced by Mr. Chabot in the 106th Congress and a bill virtually identical to H.R. 338 was introduced by Mr. Barr in the 107th Congress. In the last Congress, the Commercial and Administrative Law Subcommittee, of which Mr. Barr was Chairman, held a hearing on this measure's predecessor at which a broad political spectrum of witnesses testified in strong support of the legislation. The bill was ordered favorably reported by our Subcommittee as well as by the full Committee without amendment by voice vote. Thereafter, the House, under suspension of the rules, passed the bill without amendment by voice vote in October of last year. Unfortunately, the Senate did not consider the bill prior to the conclusion of the 107th Congress.

It is against this substantial background, that we will today consider H.R. 338.

Mr. CANNON. I now turn to my colleagues in the minority. Would anyone like to make an opening statement?

Thank you, Mr. Nadler.

The gentleman from New York is recognized for 5 minutes.

Mr. NADLER. Thank you, Mr. Chairman. I'm pleased to join you and to join this joint hearing of the two Subcommittees in this bipartisan effort to protect the privacy of the American people from unjustified encroachment by the Government. Whether for the protection of personally identifiable information from identity theft or other misuse, or the protection of the individual from unwarranted intrusions by the peering eyes of Government, the protection of privacy is of the utmost important. There are legitimate reasons the Government may need to gather personal information and, consistent with the protections of the fourth amendment, intrude into the zone of privacy. But every such intrusion and the justification for gathering and use of all such information must necessarily be scrutinized with care.

The legislation I have introduced with my colleague, the distinguished Chairman of the Constitution Subcommittee, the Defense of Privacy Act, and which was drafted with Mr. Barr, who is one of our witnesses today, would require precisely this form of careful

scrutiny. I think that requiring such deliberation in advance will minimize such intrusions and require that they be justified.

That this legislation is bipartisan and indeed has the support of both the Chair and Ranking Member of the Subcommittee sends an important message to every agency and to the American people. It makes clear that the right to privacy is a fundamental American right, and whether or not the courts have so found in any particular instance, it is one that as a matter of policy and principle should be protected scrupulously.

I am pleased to welcome back to the Committee two distinguished alumni: our former colleague, Representative Bob Barr, with whom I initially worked on this legislation, and Jim Dempsey, who served our Subcommittee ably as counsel under the chairmanship of Don Edwards. Although they come from very different political perspectives, their agreement on this particular issue demonstrates that individual privacy, or to put it more precisely, individual autonomy, is a fundamental American value.

Welcome home to you both.

I have a number of concerns that I hope we can examine today. First, what are the sources of the information gathered by the Government? Are they reliable? We have been told by the Department of Justice that among other commercially available sources, credit reporting agencies and private companies such as ChoicePoint provide data to Government agencies. I find this deeply troubling. No one familiar with these sources can have confidence in the information they provide. Credit reporting agencies are notorious for providing and failing to correct inaccurate information.

This Congress has grappled with the problems people have had getting credit on appropriate terms because of these inaccuracies. Our Committee recently reported legislation introduced by the Chairman of the full Committee dealing with the problem of fraudulent involuntary bankruptcies, which, although dismissed, remain on the targeted individual's credit report even after they are dismissed.

ChoicePoint people, you will remember, came under scrutiny following the 2000 election when it became known that its inaccurate lists illegally disenfranchised a large number of Florida voters, possibly altering the outcome of the Presidential election. If national security or law enforcement agencies are using information from these sources, we should be deeply concerned.

Second, is the Government properly protecting personal identifiable—personally identifiable information? In those cases where the Government has a legitimate need to collect such information, it's vulnerability to improper use either by another agency not entitled to use it or by private individuals who want to use that information for their own often illegal purposes would be intolerable. In some cases that information is required to be made public by law. Section 107 of the Bankruptcy Code, for example, places every aspect of a debtor's life on the Internet, making these most vulnerable of Americans even more vulnerable to the unscrupulous.

Third, does the Government have the right or a legitimate need for the information? High-tech dragnets such as the Total Information Awareness, now renamed the Terrorism Information Awareness program, would enable the Government to pore through the

personal information of millions of Americans guilty of nothing more than using a credit card, buying an airplane ticket, or taking a book out of the library without any reason to suspect that person of so much as jaywalking. Whatever name they may come up for it, we should be deeply concerned with this initiative. Moreover to the extent that this information might be shared with law enforcement agencies that would otherwise require a warrant to obtain it, the program threatens the whole underpinning of our rights under the fourth amendment.

So I welcome our witnesses and the opportunity to assess these important issues, and I look forward to a productive and informative discussion. I thank you, Mr. Chairman, and I yield back the balance of my time.

Mr. CANNON. I thank you, Mr. Nadler.

[The prepared statement of Mr. Nadler follows:]

PREPARED STATEMENT OF THE HONORABLE JERROLD NADLER, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW YORK

Thank you, Mr. Chairman. I am pleased to join you in this bipartisan effort to protect the privacy of the American people from unjustified, encroachments by the government. Whether for the protection of personally identifiable information from identity theft or other misuse, or the protection of the individual from unwarranted intrusions by the peering eyes of government, the protection of privacy is of the utmost importance.

There are legitimate reasons why the government would need to gather personal information and, consistent with the protections of the Fourth Amendment, intrude into the zone of privacy, but every such intrusion, and the justification for gathering, and use of, all such information, must necessarily be scrutinized with care.

The legislation I have introduced with my colleague, the Distinguished Chairman of the Constitution Subcommittee, the "Defense of Privacy Act," would require precisely this form of careful scrutiny. I think that requiring such deliberation in advance will minimize such intrusions and require that they be justified.

That this legislation is bipartisan, indeed it has the support of the Chair and Ranking Member of our Subcommittee, sends an important message to every agency and to the American people. It makes clear that the right to privacy is a fundamental American right and, whether or not the courts have so found in any particular instance, it is one that as a matter of policy and principle should be protected scrupulously.

I am pleased to welcome back to the Committee two distinguished alumni: our former colleague, Representative Bob Barr, with whom I initially worked on this legislative endeavor, and Jim Dempsey, who served our Subcommittee ably as Counsel under the Chairmanship of Don Edwards. Although they come from very different political perspectives, their agreement on this particular issue demonstrates that individual privacy—or to put it more precisely, individual autonomy—is a fundamental American value. Welcome home to you both.

I have a number of concerns that I hope we can examine today.

First, what are the sources of the information gathered by the government? Are they reliable? We have been told by the Department of Justice that, among other commercially available sources, credit reporting agencies and private companies such as ChoicePoint, are providing data to government agencies. I find this deeply troubling.

No one familiar with these sources can have confidence in the information they provide. Credit reporting agencies are notorious for providing, and failing to correct, inaccurate information. This Congress has grappled with the problems people have had getting credit on appropriate terms because of these inaccuracies. Our Committee recently reported legislation, introduced by the Chairman of the Full Committee, dealing with the problem of fraudulent involuntary bankruptcies which, although dismissed, remain on the targeted individual's credit report. ChoicePoint, people will remember, came under scrutiny following the 2000 election when it became known that its inaccurate lists illegally disenfranchised large numbers of Florida voters, possibly altering the outcome of the Presidential election. If national security or law enforcement agencies are using this information, we should be deeply concerned.

Second, is the government properly protecting personally identifiable information? In those cases where the government has a legitimate need to collect such information, its vulnerability to improper use, either by another agency not entitled to use it, or by private individuals who want to use that information for their own, often illegal, purposes, is intolerable. In some cases, that information is required to be made public by law. Section 107 of the Bankruptcy Code, for example places every aspect of a debtor's life on the Internet, making these most vulnerable of Americans even more vulnerable to the unscrupulous.

Third, does the government have the right, or a legitimate need, for the information? High-tech dragnets, such as the Total Information Awareness—now renamed the Terrorism Information Awareness program—would enable the government to pour through the personal information of millions of Americans guilty of nothing other than using a credit card, buying an airplane ticket, or taking a book out of the library, without any reason to suspect that individual of so much as jaywalking. Whatever name they come up for it, we should be deeply concerned about this initiative. Moreover, to the extent that this information might be shared with law enforcement agencies that would otherwise require a warrant to obtain it, the program threatens the whole underpinning of our rights under the Fourth Amendment.

So I welcome our witnesses, and the opportunity to assess these important issues, and I look forward to a productive and informative discussion.

Thank you, Mr. Chairman. I yield back the balance of my time.

Mr. CANNON. Mr. Chabot, do you have an opening statement?

Mr. CHABOT. I do. Thank you very much.

Mr. CANNON. The gentleman is recognized for 5 minutes.

Mr. CHABOT. Thank you.

First I want to thank you, Mr. Chairman, for your leadership and your willingness to hold this joint hearing on the Defense of Privacy Act, and as has been done previously, we want to welcome back our colleague Mr. Barr, who served with great distinction on this Committee on the Judiciary Committee for four terms. And we sat next to each other and often had an opportunity during Committee meetings to discuss the issues that were going on, and he was one of the more active Members. And we really do miss you here, Bob, and hope that at some point that you'll be back and join us again.

I want to also thank my Ranking Member Mr. Nadler for cosponsoring this legislation. It's fair to say that many of the judiciary Committees philosophically have a tendency to have us at odds on various issues even though we get along very well personally. But this is one piece of legislation——

Mr. NADLER. A few issues, Mr. Chairman.

Mr. CHABOT. A few. But we're pleased that this one we're able to cosponsor together and believe that it's important that we do protect the privacy rights of the American people.

Today's hearing is necessary because Federal agencies too often promulgate rules and dictate policy without consideration for the ultimate ramifications on the privacy of the American people. Privacy should not be a partisan issue. Privacy is a value that's important to all citizens whether they be Republicans or Democrats, whether they are liberal or conservative. It's really an intrinsic American value. The right of Americans to live free of excessive Government intrusion is a long-established principle in our Nation's history. Many have interpreted personal privacy as one of the blessings of liberty, secured in the Preamble of our Constitution. Certainly the Bill of Rights established important privacy protections.

Throughout our Nation's history, the Supreme Court has placed a high value on these rights as well. In 1886, Justice Clark opined

for the Court in *Boyd* v. *United States* that the doctrines of the fourth and fifth amendments, quote, "apply to all invasions on the part of the Government and its employees of the sanctity of a man's home and the privacies of life," unquote. More importantly, in his concurring opinion, in *Katz* v. *United States*, Justice Harlan succinctly stated that the fourth amendment provided citizens, quote, "a reasonable expectation of privacy," unquote.

When I first introduced the Defense of Privacy Act back in the 106th Congress, I did so because of an increasing concern that this reasonable expectation is too often an afterthought in the regulatory process. We have seen attempt after attempt by Federal agencies to implement ominous regulations that allow the Government to invade the privacy of American citizens. From financial information to medical records, the Federal Government has sought access to highly sensitive information without regard to the privacy implications.

The Defense of Privacy Act provides a straightforward solution to this problem. The legislation would, for the first time, require Federal agencies to assess the privacy implications of their proposed rules or regulations. Through this process, we would shine a light on the potentially negative impact of Government regulations on personal privacy, at the same time encouraging Federal agencies to more fully consider the merits of each proposal and review less intrusive alternatives.

This legislation is particularly relevant today. Significant technological advancements have prompted a flurry of Government proposals to employ new tools to effectively fight crime or combat terrorism. While some of these programs may ultimately prove useful and provide legitimate information to the Government, Congress and the Administration must also work to protect the privacy rights of law-abiding Americans, especially where the collection and dissemination of personally identifiable information is concerned.

In recent years we have heard a steady stream of reports about programs or policies in both the public and private sector that raise privacy concerns, from reports of drastic increases in identity theft to Government proposals like the FDIC's so-called "Know Your Customer" regulations, or, as some of us refer to it, the "Spy on Your Customer" regulations, and data-mining systems like the FBI's Carnivore that I know Mr. Barr had spoken and acted very actively when he was on this Committee. So we recognize that this is not an easy task we have before us today, and it will not get any easier in the future. Yet passing this common-sense legislation is a good first step. Requiring all Federal agencies to assess privacy implications of proposed rules and regulations will elevate the issue of privacy protection and generate important debate, thus strengthening the rights of every American.

I look forward to hearing the testimony from our distinguished witnesses here today, and I yield back the balance of my time.

Mr. CANNON. I thank you, Mr. Chabot.

[The prepared statement of Mr. Chabot follows:]

PREPARED STATEMENT OF THE HONORABLE STEVE CHABOT, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OHIO

First, I want to thank you, Chairman Cannon, for your tremendous leadership and willingness to hold this joint hearing on the *Defense of Privacy Act*. Today's hearing is necessary because federal agencies too often promulgate rules and dictate policy without consideration for the ultimate ramifications on the privacy of the American people.

Privacy is not a partisan issue. Privacy is a value important to ALL citizens—Republican or Democrat, liberal or conservative. It is an intrinsic American value.

The right of Americans to live free of excessive government intrusion is a long-established principle in our nation's history. Many have interpreted personal privacy as one of the "Blessings of Liberty" secured in the Preamble to our Constitution. Certainly, the Bill of Rights established important privacy protections.

Throughout our nation's history, the Supreme Court has placed a high value on these rights as well. In 1886, Justice Clark opined for the Court in *Boyd* v. *the United States* that the doctrines of the Fourth and Fifth Amendments "apply to all invasions on the part of the government and its employees of the sanctity of a man's home and the privacies of life."

More recently, in his concurring opinion in *Katz* v. *United States*, Justice Harlan succinctly stated that the Fourth Amendment provided citizens a "reasonable expectation of privacy."

When I first introduced the *Defense of Privacy Act* in the 106th Congress, I did so because of an increasing concern that this "reasonable expectation" is, too often, an afterthought in the regulatory process. We have seen attempt after attempt by federal agencies to implement ominous regulations that allow the government to invade the privacy of American citizens. From financial information to medical records, the federal government has sought access to highly sensitive information without regard to the privacy implications.

The *Defense of Privacy Act* provides a straight-forward solution to this problem. The legislation would, for the first time, require federal agencies to assess the privacy implications of the proposed rules or regulations. Through this process, we would shine a light on the potentially negative impact of government regulations on personal privacy—at the same time, encouraging federal agencies to more fully consider the merits of each proposal and review less intrusive alternatives.

This legislation is particularly relevant today. Significant technological advancements have prompted a flurry of government proposals to employ new tools to effectively fight crime and combat terrorism. While some of these programs may ultimately prove useful and provide legitimate information to the government, Congress and the Administration must also work to protect the privacy rights of law-abiding Americans—especially where the collection and dissemination of personally identifiable information is concerned.

In recent years, we have heard a steady stream of reports about programs or policies in both the public and private sector that raise privacy concerns—from reports of drastic increases in identity theft to government proposals like the FDIC's "Know Your Customer" regulations and data-mining systems like the FBI's "Carnivore." So, we recognize that this is not an easy task today, and it will not get any easier in the future. Yet, passing this common-sense legislation is a good first step. Requiring all federal agencies to assess privacy implications of proposed rules and regulations will elevate the issue and generate important debate—strengthening the rights of every American.

I look forward to hearing the testimony from our distinguished witnesses today.

Mr. CANNON. We'd like to also recognize Mrs. Blackburn from Tennessee and Mr. Scott from Virginia.

Without objection, all Members may place their opening statements in the record at this point. Is there objection? Hearing none, so ordered.

Without objection, the Chair will be authorized to declare recesses of the Subcommittee today at any point. Hearing none, so ordered.

On unanimous consent I ask that Members have 5 legislative days to submit written statements for inclusion in today's hearing record.

I'm now going to introduce our witnesses. We expect Senator Grassley to join us. He's apparently in a hearing, and so we will come back and introduce him when he arrives.

Joining Senator Grassley, or maybe we should say after we hope Senator Grassley joins the rest of us, we'll hear from our esteemed colleague and probably hear first from you, unless Senator Grassley comes in soon, Bob Barr. Bob, as you know, chaired this Subcommittee, which I am honored to succeed him in this position, during the 107th Congress, and, in fact, he authored the H.R. 338's predecessor in the last Congress.

It's a great pleasure to welcome you back, Bob.

Over the course of his four terms in Congress, representing Georgia's Seventh District, Mr. Barr served on the Financial Services and Government Reform Committees in addition to the Judiciary Committee. As one of the Nation's leading privacy hawks, it's particularly appropriate for him to share his thoughts on this legislation. He appears today as the 21st Century Liberties Chair for Freedom and Privacy at the American Conservative Union.

Our next witness is Jim Dempsey, another Judiciary Committee alum, whom we also welcome back. Mr. Dempsey is currently the executive director of the Center on Democracy and Technology. That's got to be one of the coolest jobs on the face of the Earth, by the way.

Mr. DEMPSEY. Yes, sir, it is.

Mr. CANNON. If you need some bipartisan—I'd love to do something with you guys—where he specializes in privacy and electronic surveillance issues.

Before joining the center, Mr. Dempsey was the deputy director of the Center for National Security Studies and also served as special counsel to the National Security Archive, a nongovernmental organization that uses the Freedom of Information Act to gain the declassification of documents pertaining to U.S. foreign policy.

From 1985 to 1994, Mr. Dempsey was assistant counsel to the House Judiciary Subcommittee on Civil and Constitutional Rights, the precursor to the Subcommittee on the Constitution, which is jointly holding this hearing with us today.

Mr. Dempsey obtained his undergraduate degree from Yale College and his law degree from Harvard Law School.

Our final witness is Laura Murphy. Laura is the director of the Washington office of the American Civil Liberties Union, the Nation's oldest and largest civil liberties organization. As Washington office director, she directs the national legislative and executive branch priorities on behalf of the 250,000-member organization.

The first woman and first African American to hold the position of Washington office director, Ms. Murphy had previously worked for the ACLU as a lobbyist for more than 3 years during which she was instrumental in the passage of the Voting Rights Act extension of 1982.

She was a development director in the southern California ACLU affiliate and has worked for five elected officials in the State; State, municipal and Federal levels. And I have worked with her in particular, along with Mr. Barr, on the Patriot 1. Interesting, we now call it Patriot 1 because we have a Patriot 2 coming maybe, or at least there'll be an attempt. I suspect the Patriot 2 will be a—just

some minor technical corrections and not some of the major changes that some want.

But it was a pleasure working with you, and I welcome you here today, Ms. Murphy.

Ms. MURPHY. Thank you.

Mr. CANNON. I extend to each witness my warm regards and appreciation for your willingness to be at today's hearing. In light of the fact that your written statements will be included in the hearing record, I request that each of you limit your oral remarks to 5 minutes. Accordingly, please feel free to summarize or highlight the salient points of your testimony.

You will note, and I think you all have had experience, there is a little device that has a green and then a yellow and a red light. The yellow means you have 1 minute remaining. To be consistent I will tap when the red light goes on. That doesn't mean stop. It means wrap up, if you will. During questioning I try to be very careful to remind people when time is up on an even-handed basis. Again, if you're answering the question, a tap just means that if you'd finish your answer, we would appreciate it.

Senator Grassley, welcome. Would you like to join us at the table, Senator? We would all love to have the obscurity which you enjoy, which is national fame and recognition. I have not introduced you, so, Mr. Grassley, if you would allow me.

I'm honored to introduce today particularly our senior Senator from Iowa, Senator Chuck Grassley. In addition to having the distinction of being the only working family farmer in the United States Senate, Senator Grassley currently chairs the Senate Finance Committee and plays an active role on the Senate Judiciary Committee.

We understand that he has just returned from a Senate judicial confirmation hearing. We hope that was successful. So we're especially appreciative that he was able to adjust his busy schedule in order to participate in today's hearing.

And with that, Senator, if you would like to go ahead and speak, we would appreciate hearing from you.

STATEMENT OF THE HONORABLE CHARLES E. GRASSLEY, A UNITED STATES SENATOR FROM THE STATE OF IOWA

Senator GRASSLEY. Thank you very much, Mr. Chairman. Congressman King, my fellow Congressman from Iowa. First of all, I appreciate very much the introduction. If my son Robin heard that, he'd say, Dad, why don't you tell them I do all the work? So Robin Grassley does most of the work on the family farm.

Mr. Chairman and Members of the Subcommittee, I thank you for this opportunity to testify on a very important topic of privacy. In this post-September 11 world, the Government must do everything within its power and within the law to protect our citizens and country, but more and more, this stepped-up protection involves intrusion of private lives. Some of them are just plain inconveniences, but some of them approach violation of fundamental rights.

Justice Brandeis noted in 1928, quote, the right to be left alone is the right that Americans cherish most, or at least more than most of any right, is what he said. It's my belief that one of the

most important jobs we as legislators and overseers of the executive process do is vigorously guard and protect the right to be left alone. I'd like to focus my remarks on this important oversight aspect of our job and specifically on the Terrorist Information Awareness program, or TIA, that the Defense Department is presently researching.

Power can be abused if put in the wrong hands. That's why checks on power are critical for privacy. A prosecutor can go too far in pressing a case, harassing and embarrassing a private person. So judges and defense counsel are a critical check on prosecutorial power. Likewise, an overzealous investigator can dig too deeply into private lives. So the courts, under authority of the Constitution, are there to restrain undue probing. Even intelligence officials' powers are checked by the Foreign Intelligence Surveillance Act and the secret court that enforces that act. Without these checks, even a good-meaning public official can overreach and exploit our deeply cherished privacy.

But in some instances, there aren't systemic checks in place. A public official working deep within the bowels of a Government agency may be able to burrow into private information of people with little or no oversight. So H.R. 338 appears to focus on some of these situations where new administrative rules could create opportunities for unwarranted intrusion into privacy. The bill's impact statement requirement would force careful consideration of appropriate safeguards to protect civil liberties. It is important that this process doesn't become too cumbersome, create new bureaucracies or cause unnecessary delays. We need a careful, but nimble Government to fight terrorism. I look forward to listening to the debate on the bill in the coming weeks.

It is in these situations where there's no obvious safeguard that the Congress must provide rigorous oversight of the executive branch and do that to protect the public, and also the public's cherished right to privacy, and do that against unwarranted Government intrusions. I describe one such incident where I've been involved in heavy oversight to protect civil liberties.

Many of you may know about the Defense Department's TIA program that's designed to test technologies that collect information from private and public databases and try in turn to find trends that could signal threats against our country. This program's being run under DARPA, the DOD's unit that created the Internet. Like many people, I have been concerned that TIA would be used to invade the privacy of Americans by snooping around our bank accounts, personal Internet computers, phone records, and a lot of other things you can think of. In November of last year, I asked the Department of Defense inspector general to look into the reasons for TIA and to make sure that there are controls in place to ensure that it's used only for foreign intelligence purposes and for that purpose, to protect us against terrorism and foreign threats. The inspector general's investigation is proceeding, and a formal audit of TIA should be finished by the fall.

In January of this year, Democratic Senator Ron Wyden and I were able to get an amendment attached to the Department of Defense appropriation bill that limited funding for TIA research and required congressional reporting and oversight. In a recent report

the Department of Defense seems to have embraced its role in restricting the intrusion TIA will have into people's lives and has confirmed that it will not, and has confirmed that it cannot, meddle into private information that it's not otherwise allowed access to under existing law.

After 9/11, all of us in Congress were questioning why Government failed to connect the dots and recognize terrorist activities that were interrelated. Well, it's my understanding that TIA is being researched as a tool that could potentially help connect some dots. But we have to be careful about on the one hand demanding that the Administration connect the dots and, on the other hand, putting a stop to their efforts to connect the dots. I have learned that the Department of Defense appropriation bill that's currently being debated would cut off all research funding. We need to proceed with caution. But one thing's for certain: Oversight is critical.

It is a delicate balance that Congress must strike between protecting people from terrorism and protecting people from unwarranted Government intrusion into their private lives, and in the mix must be rigorous and effective congressional oversight. You can expect that I will continue to carry the oversight torch, and I hope that each of you will as well.

I thank you for your time and focusing on a very important subject, Mr. Chairman.

Mr. CANNON. Thank you, Mr. Grassley.

[The prepared statement of Senator Grassley follows:]

PREPARED STATEMENT OF THE HONORABLE CHUCK GRASSLEY, A U.S. SENATOR FROM THE STATE OF IOWA

Chairman Cannon, Chairman Chabot, Members of the Subcommittees, thank you for the opportunity to testify on the important topic of privacy. In this post-September 11 world, the government must do everything within its powers, and within the law, to protect our citizens and country. But more and more this stepped-up protection involves intrusions into our private lives. Some of them are just inconveniences; but some of them approach violations of fundamental rights. The "right to be let alone," as Justice Brandeis noted in 1928, is the right that Americans cherish more than most any right.

It is my belief that one of the most important jobs we as legislators and overseers of the executive process do is vigorously guard and protect the right to be let alone. I'd like to focus my remarks on this important oversight aspect of our job and, specifically, on the Terrorist Information Awareness program—T-I-A—that the Defense Department is researching.

Power can be abused if put in the wrong hands. That's why checks on power are critical for our privacy. A prosecutor can go too far in pressing a case, harassing and embarrassing a private person. So judges and defense counsel are a critical check on prosecutorial power. Likewise, an overzealous investigator can dig too deep into private lives. So the courts—under the authority of the Constitution—are there to restrain undue probing. Even intelligence officials' powers are checked by the Foreign Intelligence Surveillance Act and the secret court that enforces that act. Without these checks, even a good-meaning public official can overreach, and exploit our deeply cherished privacy.

But in some instances, there aren't systemic checks in place. A public official working deep within the bowels of a government agency may be able to burrow into the private information of people with little or no oversight. H.R. 338 appears to focus on some of those situations where new administrative rules could create opportunities for unwarranted intrusions into privacy. The bill's impact statement requirement would force careful consideration of appropriate safeguards to protect civil liberties. It is important that this process doesn't become too cumbersome, create new bureaucracies, or cause unnecessary delays. We need a careful but nimble government to fight terrorism. I look forward to listening to the debate on this bill today and in the coming weeks.

It's in these situations, where there's no obvious safeguard, that the Congress must provide rigorous oversight of the Executive Branch to protect the public—and the public's cherished privacy rights—against unwarranted government intrusions. Let me describe one such instance where I've been involved in heavy oversight to protect civil liberties.

Many of you may know about the Defense Department's TIA program that's designed to test technologies that collect information from public and private databases and try to find trends that could signal threats against the United States. This program's being run under DARPA, the DOD unit that created the internet. Like many people, I've been concerned that TIA could be used to invade the privacy of Americans by snooping around in our bank accounts, personal internet computers, phone records, and the like. In November of last year, I asked the DOD Inspector General to look into the reasons for TIA and to make sure that there are controls in place to ensure that it's used only for foreign intelligence purposes to protect us against terrorism and foreign threats. The IG investigation is proceeding, and a formal audit of TIA should be finished by the Fall.

In January of this year, Senator Ron Wyden and I were able to get an amendment attached to the DOD appropriations bill that limited funding for TIA research, and required Congressional reporting and oversight. In a recent report, DOD seems to have embraced its role in restricting the intrusion TIA will have into people's lives, and has confirmed that it will not, and cannot, meddle into private information that it's not otherwise allowed access to under the law.

After 9/11, all of us in the Congress were questioning why the government failed to "connect the dots" and recognize terrorist activities that were interrelated. Well, it's my understanding that TIA is being researched as a tool that could potentially help connect some dots. We have to be careful about on the one hand demanding that the administration connect the dots—and on the other hand putting a stop to their efforts to connect the dots. I have learned that the DOD appropriations bill that's currently being debated would cut off all research funding—we need to proceed with caution here. But one thing's for certain, oversight is critical.

It's a delicate balance that Congress must strike between protecting people from terrorism, and protecting people from unwarranted government intrusions into their private lives. In the mix must be rigorous and effective congressional oversight. You can expect that I will continue to carry the oversight torch, and I hope that each of you will too.

I thank you for your time, and for focusing on this important topic.

Mr. CANNON. We recognize your schedule is busy. If you need to leave, you certainly don't need to ask. But have you got a little bit of time to do questions with us?

Senator GRASSLEY. I'll try, yes.

Mr. CANNON. Okay. No compulsion here, but we really appreciate your insights into that situation.

Senator GRASSLEY. I really need to go back to Judiciary.

Mr. CANNON. Would you please get something done over there? I'm not sure how you're going to do that, but you have our support, maybe even our prayers.

Mr. GRASSLEY. If we had your Rules Committee, we could do a lot.

Mr. CANNON. Thank you, Senator Grassley.

Mr. Barr.

STATEMENT OF THE HONORABLE BOB BARR, 21ST CENTURY LIBERTIES CHAIR FOR FREEDOM AND PRIVACY, AMERICAN CONSERVATIVE UNION

Mr. BARR. Thank you very much, Mr. Chairman and Mr. Chairman Chabot. It's a tremendous honor to be here today with you and distinguished Ranking Member and good friend Mr. Nadler, whom—with whom I've had the pleasure in months since I left the Congress to share some podiums to discuss these very issues. It is a tremendous honor to be before you and Mr. Scott, with whom I worked very closely. It was an honor. I look up to him as a mentor,

coming as he does from Harvard and being very well versed in so much of what went on in the Judiciary Committee, and I enjoyed working with him very closely on many of the pieces of legislation. Colonel, so wonderful to see you today. Mr. Coble, my good friend and colleague; and Mr. Flake, from the great State of Arizona.

It's wonderful to be with you all today and to think as we proceed with this hearing of the many issues on which we worked together constructively, Democrat, Republican, those from a more liberal persuasion and a more conservative one. And that really is, as Mr. Chabot indicated, Mr. Cannon indicated, Mr. Nadler indicated in their opening remarks, is really the hallmark of this legislation.

It is an honor to be back before the Subcommittee, and I will submit my written remarks for inclusion, as the Chairman indicated, in their entirety in the record, and appreciate that courtesy being extended.

Let me speak to just a couple of points and then listen to Mr. Dempsey, for whom I have the highest regard on these matters of privacy and Government power, and I have had the pleasure of working with him on many occasions, and after him, to Ms. Murphy, who has really been a stalwart not only here in Washington, D.C., but across the country in working on these tremendously important privacy and other civil liberties matters. And it is an honor to appear today with them, as it was with my good friend from my native State of Iowa, Senator Grassley.

Mr. Chairman, while the world of George Orwell's 1984 face crime and thought crime and the world of Minority Report's precrime detention and arrest are not fully upon us, their specter is so close that it casts a shadow over our Nation, and we need to do everything within our power to ensure that the mechanisms that we read about in those novels and in those movies do not become the reality of TIA gone wild or CAPS II gone astray, or any of the other myriad programs such as Project Carnivore that I think Mr. Chabot indicated we worked on years ago do not obtain the hold on our society that some, perhaps in the minority, but some in our society would like them to do. If we allow that to happen, then indeed we will look back on these days of vast Government power as the good old days when there was at least some freedom and some privacy left, and I know none of us here in this room today want to see that happen.

This piece of legislation, carefully crafted as I know it is, very well thought out as it obviously is, is a very, very modest piece of legislation. Some might ask on the outside why bother with such a modest piece of legislation, foregoing as it does a direct attack, so to speak, on some of the mechanisms that we're all familiar with? I think it's important to make this small, but significant step, as Chairman Chabot described it, as a good first step because we do want to tread carefully.

None of us have a desire to thwart the Government's legitimate and paramount interest in fighting the war against terrorism and other criminal activity. We certainly want to make sure that what we do to ensure that privacy is protected, and in those instances where it has been threatened or curtailed, it is made whole again, we certainly want to make sure that those do not come at the expense of legitimate law enforcement, legitimate antiterrorism ef-

forts or legitimate foreign intelligence-gathering, analysis, coordination and dissemination efforts.

And that is why I think this first step is a very, very appropriate one. It will send a very important message not just to the American people, but to the courts and to the executive branch that we in the Congress, that you in the Congress, care deeply about privacy, and that you are taking steps, concrete steps, through this legislation to begin the process of ensuring that privacy is fully recognized and protected as one of the foundational principles underlying our Bill of Rights.

The legislation does in many respects, if not precisely, mirror legislation that Mr. Chabot, as was indicated, introduced in the 106th Congress and as I introduced with the support of many on these two panels in the 107th Congress. I stand ready to assist in any way possible with this legislation not just today, but in the months ahead and would be glad to answer any questions or engage in any colloquies or discussions today as we look at specific aspects of the legislation. Thank you, Mr. Chairman.

Mr. CANNON. Thank you, Mr. Barr.

[The prepared statement of Mr. Barr follows:]

PREPARED STATEMENT OF THE HONORABLE BOB BARR

I am pleased to offer my views today on behalf of the American Conservative Union at this joint hearing of the Subcommittee on Commercial and Administrative Law and Subcommittee on the Constitution to examine the Defense of Privacy Act, H.R. 338, introduced by Representative Chabot, the distinguished Chairman of the Subcommittee on the Constitution, and Representative Nadler, its ranking member. This legislation also enjoys the support of my good friend Representative Cannon, the distinguished Chairman of the Subcommittee on Commercial and Administrative Law, who I am very pleased to see has so ably taken up the gavel that I was once honored to hold.

I am particularly pleased that you have taken up this issue, Chairman Cannon, as bipartisan work on this issue—and on this important legislation—were, as you know, among the issues most dear to my heart when I sat where you are sitting now. I now appear before you to represent the American Conservative Union, the nation's oldest conservative lobbying organization, which expresses its strong endorsement of this legislation. I hope we can, together, speedily send this good government initiative on its way through the House and ultimately to the President's desk.

It is clear that those of us who support this legislation, both in and out of Congress, do not agree on every issue. In fact, however, many observers have been particularly impressed by the political diversity of the bill's supporters, and I am pleased to be part of a distinguished panel which also spans the conventional ideological spectrum.

Supporters of this legislation share a commitment to protecting the privacy cherished by American citizens—a value increasingly imperiled in an information age in which personal information has become a commodity that is captured and compiled, manipulated and misused, bought and sold in ways not even imaginable just a few years ago. The sphere of privacy, which Justice Brandeis eloquently described as the "right to be let alone," is not only rapidly diminishing, it is increasingly penetrable. Special care is necessary to ensure that personal information remains personal, absent a sound reason to treat it otherwise. This value is neither Republican or Democratic; liberal or conservative, it is truly an *American* value; one that remains a the heart of our way of life and of our Bill of Rights.

H.R. 338 takes the first—necessary—step toward protecting the privacy of information collected by the federal government. While some have decried the loss of personal privacy by private companies, (and this is indeed a matter of grave concern), it must be emphasized that government alone has the *authority* to *compel* the disclosure of personal information; and unlike a private commercial gatherer of personal data, the government can put you in jail based on what it uncovers. For this reason, the government has an obligation to exercise great *responsibility* when enacting policies that undermine privacy rights.

The Defense of Privacy Act requires that rules noticed for public comment by federal agencies be accompanied by an assessment of the rule's impact on personal privacy interests, including the extent to which the proposed rule provides notice of the collection of personally identifiable information, what information will be obtained, and how it is to be collected, maintained, used and disclosed. The measure further provides that *final* rules be accompanied by a *final* privacy impact analysis, which indicates how the issuing agency considered and responded to privacy concerns raised by the public, and explains whether the agency could have taken an approach less burdensome to personal privacy.

Unlike existing laws that protect against the disclosure of information *already* obtained by the federal government, the Federal Agency Protection of Privacy Act provides *prospective* notice of a proposed rule's affect on privacy *before* it becomes a binding regulation. Together with a wide and diverse array of co-sponsors, I introduced an earlier version of this measure last Congress—H.R. 4561, the Federal Agency Protection of Privacy Act, which passed the full House by a voice vote under suspension of the rules. Unfortunately, the Senate did not take up the measure with the rush of business at the end of a busy 107th Congress, but I am confident that with such broad support we will get the job completed this year.

Like that earlier measure, H.R. 338 specifically articulates the principles that should guide agency action when rules that impact privacy are promulgated: 1) the public should have notice that a rule provides for the collection of personally identifiable information and how the agency will collect, maintain, use and disclose that information; 2) individuals should have access to information that pertains to them and an opportunity to correct inaccuracies; 3) agencies should take steps to prevent information collected for one purpose from being used for another purpose; and 4) agencies should take steps to provide *security* for such information.

Importantly, H.R. 338 permits individuals who are adversely affected by an agency's failure to follow its provisions to seek judicial review pursuant to the provisions of the Administrative Procedure Act. In this respect, the bill tracks the administrative innovations of 1996 amendments to the Regulatory Flexibility Act, which provided for the judicial review of rules issued without regard to their impact on small businesses. I can say, without hesitation, that privacy is no less important to American citizens than regulatory burdens are to American businesses, and this measure helps address these concerns.

Finally, I want to emphasize that H.R. 338 will *not* unduly burden regulators *nor* will it hinder law enforcement or foreign intelligence gathering. The Defense of Privacy Act will apply the best antiseptic—*sunshine*—to the federal rulemaking process by securing the *public's right to know* about how rules will affect their personal privacy while ensuring that citizens have the opportunity not only to critique the substance of a rule, but to do so with an understanding of the reasoning and justification upon which the rule was predicated.

On behalf of the American Conservative Union, I thank the Committee for this opportunity to express our strong support for this important legislation.

Mr. CANNON. Mr. Dempsey, you are recognized for 5 minutes.

STATEMENT OF JAMES X. DEMPSEY, EXECUTIVE DIRECTOR, CENTER FOR DEMOCRACY & TECHNOLOGY

Mr. DEMPSEY. Thank you, Mr. Chairman and Chairman Chabot and Mr. Nadler, Members of the two Committees. It is a privilege to be here today, especially to share the witness table with Senator Grassley and Mr. Barr and Ms. Murphy, three of the leading advocates and supporters of privacy in this country.

The Center for Democracy and Technology is here today in strong support of H.R. 338. The legislation has in it a concept; the core of it is the privacy impact assessment, and this is clearly a concept whose time has come. Even though this legislation was not enacted in the 106th Congress or last year, the principle is being implemented already in Government agencies, is being adopted by the Congress. In the E-Government Act, which was adopted last year, that legislation included a requirement for privacy impact assessments when the Government was procuring new computer systems. And when Congress also last year adopted the Homeland Se-

curity Act, it took the privacy impact assessment concept and it included it in the Homeland Security Act and gave that responsibility to the privacy officer in that agency.

So H.R. 338 would fully deploy, so to speak, this concept across the Government. We've seen the idea being picked up already, and it's now time to apply it across the board to Federal agency rulemaking.

Now, the concern might be raised that this would be an encumbrance to the Federal bureaucracy, or that it would impose unnecessary costs. I want to stress a point that Chairman Cannon made in his opening statement, which was that last year the Congressional Budget Office studied this legislation and in its estimate concluded that it would not impose any significant cost or require any significant expenditure, and pointed out that only a small percentage of the Federal regulations would actually require a full privacy impact assessment.

And I would like to stress that I think that in many ways, this legislation can end up saving money and actually streamlining the realization of Government programs and the achievement of legitimate Government interests, and that's because the legislation forces agencies to focus on the privacy concerns at the point when it can make the most difference; that is, at the design phase, at the initial phase when the Government is deciding to initiate through regulation a new collection of information. That's the time to surface problems and to correct them. It could end up saving money and avoiding litigation.

I know just one example. Last year a Government contractor lost or suffered a security breach. Five hundred thousand records of military personal and retired Active Duty and retired military personal and their families were stolen by computer because of poor computer security practices from computer systems run by a contractor. The Government and the contractor are now having to spend hundreds of thousands, if not millions, of dollars notifying those people and trying to rectify that damage. And if the security issues associated with that information had been surfaced at the outset, that could have been avoided.

The legislation creates a public input mechanism so that groups like the American Conservative Union and the ACLU and CDT can comment on rulemaking and put suggestions; making suggestions, for example, to use an identifier other than the Social Security number, which we know has gotten out of hand, and is the key to identity theft, and maybe a system could be designed to avoid that so we can build privacy into the design of data collection.

Now, I would just point out that there is one issue which Senator Grassley alluded to, the Chairman in his opening statement alluded to, that I think is actually not covered by this legislation, which desperately needs being addressed, and that is the increasing use by the Government of commercial databases where the Government buys the information or subscribes to it from the private sector, doesn't mandate the disclosure by rulemaking, doesn't take the information into its own database, so it never really becomes subject to the Privacy Act. The FBI has reported that its use of these commercial databases has grown by 9,600 percent since 1992. Congress needs to figure out what's going on there. They

need to require the agencies to disclose how they are using this data and to walk through many of the questions that are in this legislation.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Dempsey follows:]

PREPARED STATEMENT OF JAMES X. DEMPSEY

Chairman Cannon, Chairman Chabot, Members of these two Subcommittees, thank you for the opportunity to testify today on H.R. 338, the Defense of Privacy Act. We commend you for your attention to the important privacy issues surrounding the government's collection and use of personal information. We offer here today our strong support for the Defense of Privacy Act. In addition, we suggest some further steps Congress should take to ensure fairness in the government's collection or use of personal information, particularly with regard to government access to commercial databases and the possible use of "data mining" techniques. We look forward to ongoing work with you on these issues.

I. SUMMARY

The federal government has many legitimate needs for personal information, ranging from administration of benefits programs to tax collection to winning the war on terrorism. Especially in light of the digital revolution, this government demand for information brings with it heightened risk to privacy and the associated values of Fair Information Practices. The Defense of Privacy Act would put in place an important process to protect Americans' privacy against unnecessary or unwise government intrusions. The Act requires government agencies to closely examine the privacy impact of their rules and regulations and to consider alternative ways to accomplish their objectives while minimizing any adverse privacy impact. The Act focuses on the point when careful consideration of privacy could do the most good: at the beginning of the regulatory process.

The Defense of Privacy Act serves as a sound complement to Section 208 of the E-Government Act of 2002, which requires that federal agencies conduct privacy impact assessments whenever they purchase a new information technology or initiate a new collection of personally identifiable information. However, we note with dismay that the Office of Management and Budget (OMB) has failed to issue guidance to agencies on performing the privacy impact assessments under the E-Gov Act. We urge the Subcommittees to send a strong message to OMB that it should promptly issue guidance to the agencies on the E-Gov Act privacy impact assessment process.

While adoption of the Defense of Privacy Act and full implementation of the E-Gov Act would be important steps, further congressional action is needed to address a new problem: the growing use by federal law enforcement and intelligence agencies of sensitive, personal data about Americans held by the private sector or collected by government agencies for purposes other than law enforcement or intelligence. With growing frequency, the government does not compel disclosure of private sector data but rather purchases access to it. Since this information is not collected under a regulation, it would not be subject to the Defense of Privacy Act. Agencies are developing new "data mining" technologies that would seek evidence of possible terrorist preparations by scanning billions of everyday transactions, potentially including a vast array of information about Americans' personal lives, such as medical information, travel records, credit card and financial data, and government data initially collected for non-law enforcement purposes. Contrary to some reports, research on data mining continues under the auspices of the Total (now Terrorism) Information Awareness (TIA) project at the Pentagon's Defense Advanced Research Projects Agency. And even if TIA funding were zeroed out, the development of data mining would go on commercially or at other agencies. Government implementations of this uniquely intrusive technology should not go forward without explicit congressional authorization based on (i) a finding of effectiveness, (ii) guidance for implementation, and (iii) oversight. CDT urges the Congress to develop, first, a structure or criteria for evaluating the effectiveness of particular uses of data analytics technology and then, for specific situations where the use of such techniques are found to be effective, guidelines and an oversight process for protecting privacy and due process. CDT offers its assistance in that process.

II. THE DEFENSE OF PRIVACY ACT AND PRIVACY IMPACT ASSESSMENTS

A. The Defense of Privacy Act

CDT strongly supports enactment of H.R. 338, the Defense of Privacy Act, introduced this Congress by Chairman Chabot and cosponsored by Representatives Boucher and Nadler. The bill would require agencies to conduct privacy impact analyses for both new and existing agency rules and regulations. Importantly, it would provide a judicial review mechanism to ensure enforcement. For the same reasons that we supported former Representative Barr's Federal Agency Protection of Privacy Act, which passed the House of Representatives in the last Congress but was never taken up by the Senate, we believe that H.R. 338 provides a sound approach for enhancing privacy protections for the federal government's collection and use of personally identifiable information.

The privacy impact analyses required by the Defense of Privacy Act will greatly improve the regulatory process. They will force agencies to consider issues they have often overlooked in issuing regulations, namely the privacy implications. Agencies would have to consider ways to reduce the privacy impact of regulations. And they would have to systematically justify their decisions to collect personally identifiable information.

Specifically, the bill requires agencies to address up front some of the basic "Fair Information Practices" that are reflected in the federal Privacy Act of 1974, such as notice to individuals of the collection of personally identifiable information, the right of individuals to access information about themselves, the opportunity to correct information, limits on use and disclosure of data for purposes other than those for which the data was collected in the first place, and appropriate security measures to protect the information against abuse or unauthorized disclosure.

These "Fair Information Practices" form part of the foundation of the Privacy Act, which was enacted in response to the creation of government computer databanks filled with personally identifiable information. (As will be discussed below, the Privacy Act has a number of exemptions and loopholes that render it less effective today than intended.) Other Fair Information Practices, which are also reflected in the Privacy Act, include limitations on the retention of data, a requirement to ensure the accuracy, completeness and timeliness of information, and the establishment of redress mechanisms for individuals wrongly and adversely affected by the use of personally identifiable information. We recommend that those additional principles be included in the Defense of Privacy Act's list of considerations that agencies must review when issuing regulations, so that the Defense of Privacy Act fully tracks the Privacy Act of 1974.

A key element of the Defense of Privacy Act is that it would require policy makers to identify and address privacy issues at the initial stages of a new project or policy—at the conceptual or design stage, before regulations are promulgated. This represents a vast improvement over current practice. It also means that the Act should not adversely interfere with agency operations. Instead, it will reduce the likelihood that any given regulatory scheme will be found to have a negative impact on privacy after it has been implemented, when it may be difficult to mitigate the impact without substantial expense, delay in the program or even litigation. The requirement that agencies periodically review existing regulations that have serious privacy implications could also benefit agency operations by identifying information collection practices that have become outdated or unnecessary and that can be dispensed with altogether.

The privacy impact analyses will not force agencies to adopt any one privacy standard. Indeed, different standards may well be appropriate for different programs dealing with information of varying sensitivity. However, having to work through a privacy impact analysis should guide an agency in acting more responsibly, and as a result this bill should lead to better regulations and fewer unnecessary privacy intrusions.

B. Failure to Fully Implement the E-Government Act

Enactment of H.R. 338 would not be the first time that Congress has directed federal agencies to analyze the privacy impact of their programs. Just last year, the E-Government Act of 2002 included a provision, Section 208, requiring federal government agencies to conduct privacy impact assessments before developing or procuring information technology or initiating any new collections of personally identifiable information. Under that legislation, a privacy impact assessment must address what information is to be collected, why it is being collected, the intended uses of the information, with whom the information will be shared, what notice would be provided to individuals, and how the information will be secured. The privacy impact assessments required under the Defense of Privacy Act complement the re-

quirements under the E-Gov Act. We urge the Subcommittees to ensure that the two Acts are congruent. Our initial thoughts are that this should be done by making the list of factors to be considered the same in both, and by making it clear that when a new collection of information is initiated by rule, the notice and comment provisions of the Defense of Privacy Act apply to the privacy impact assessment process.

The privacy impact assessments under the E-Gov Act should bring greater transparency to the IT development and procurement process, allowing Congress, citizens and advocacy groups to better scrutinize the privacy decisions of the government. And using the massive purchasing power of the U.S. government, the assessments could help to increase the marketplace for technologies that incorporate privacy "by design."

Unfortunately, privacy impact assessments for information technology procurements have only been implemented by a few agencies, despite the fact that the E-Government Act set an April 2003 deadline for implementation. The Director of OMB was supposed to issue guidelines in April for agencies on how to draft the assessments, but has failed to do so. As a result, the implementation of this important new privacy protection has been significantly pushed back. CDT is very concerned about this delay. These Subcommittees should encourage the Executive Branch to get on with implementation of the E-Gov Act. Guidance issued for privacy impact assessments under the E-Gov Act could also help agencies perform similar assessments of regulatory actions under the Defense of Privacy Act.

It is worth noting that privacy impact assessment requirements like those in the Defense of Privacy Act and the E-Government Act are not a new or uniquely American concept. Privacy impact assessments already are used in several other countries. Indeed, privacy commissioners in Canada and New Zealand have issued excellent guides or handbooks on conducting privacy impact assessments, which may assist OMB in issuing its guidance. For more information about the international experience, see *Privacy and E-Government: Privacy Impact Assessments and Privacy Commissioners—Two Mechanisms for Protecting Privacy to Promote Citizen Trust Online*, a report of the Global Internet Policy Initiative, which can be found at *http://www.gipiproject.org/practices/030501pia.pdf.*

C. Privacy Officers

We briefly mention one other important privacy protection mechanism, the Privacy Officer, now being implemented at the Department of Homeland Security. In Section 222 of the Homeland Security Act of 2002, Congress established a Privacy Officer for the Department. The Privacy Officer's statutory responsibilities include "evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Federal Government" and "conducting a privacy impact assessment of proposed rules of the Department . . . including the type of personal information collected and the number of people affected." CDT believes that every federal agency should have a statutory Privacy Officer with authorities similar to those provided under the Homeland Security Act. This officer would have the stature and expertise to effectively conduct privacy impact assessments of the kind required under the Defense of Privacy Act, and the Defense of Privacy Act would give these officers specific requirements and an enforcement mechanism to draw on in fulfilling their duties. Attempts by the Clinton Administration to create privacy officers by Executive memorandum were unsuccessful. The position needs and deserves statutory footing.

III. THE NEED FOR FURTHER CONGRESSIONAL ACTION REGARDING THE PRIVACY IMPLICATIONS OF DATA MINING AND OTHER GOVERNMENT USES OF COMMERCIAL INFORMATION

The E-Government Act's requirement that agencies issue privacy impact assessments each time they procure new information technology systems was a vital step toward making privacy a significant part of government decision-making processes. The Defense of Privacy Act addresses another major concern by requiring agencies to consider the privacy implications of their proposed and existing regulations. But there is a third set of issues not necessarily addressed by either of those provisions: "data mining" and other law enforcement and intelligence uses of commercial data and other information that was not initially collected for law enforcement and intelligence purposes. Law enforcement and intelligence agencies are increasingly buying commercial data or developing new uses of government data originally collected for non-law enforcement or intelligence purposes. A new theory of pattern-based analysis is being developed that claims the ability to review the ocean of data we generate in everyday life, potentially including a vast array of information about Americans' personal lives such as medical information, travel records and credit card and

financial data. Such techniques turn the presumption of innocence upside down. They seem to assume government access to personal information about everyone from any source. Yet this is an area where few laws, regulations or guidelines constrain the government or provide any meaningful oversight or accountability. CDT urges Congress to address this significant gap in privacy protection.

Before going into further detail, let me be clear on one point: The threat terrorism poses to our nation is imminent and grave. Our nation critically needs a more effective intelligence effort to thwart terrorism, and this effort must include new technologies for collecting and analyzing information from public and private sources. But advanced information technology, by its power to search decentralized databases, has new, grave privacy implications. Such technology must be used only if effective; it must be subject to checks and balances; it must be implemented with a focus on actual suspects, guided by the particularized suspicion principle of the Fourth Amendment; and it must be subject to executive, legislative and judicial controls. At this time, those checks and balances do not exist.

A. Access to Information Initially Collected for Purposes Other Than Law Enforcement and Intelligence

Increasingly, U.S. law enforcement and intelligence agencies are seeking access to commercial data and other personally identifiable information that was not initially collected for law enforcement and intelligence purposes. Agencies can obtain this information via subscription, through voluntarily disclosures, or under new Patriot Act authorities that authorize access under very weak standards. The Constitution as currently interpreted provides no limits on government collection of this information because courts in the pre-Internet era—not envisioning a technology that could link vast public and private databases to present a composite image of any individual—held that individuals do not have Fourth Amendment rights in personal information disclosed to third parties like banks and credit card companies in the course of business transactions.

The result is that the government faces few constraints on its ability to obtain and use this information. For years the FBI has had contracts with major companies that aggregate commercial data about individuals. According to an undated FBI presentation obtained by the Electronic Privacy Information Center, the FBI's use of "public source" information (including those proprietary commercial databases) has grown 9,600% since 1992. Other entities that collect commercial information have voluntarily provided the FBI with their databases, from grocery store frequent-shopper records to scuba diving certification records. But it is entirely unclear what, if any, guidelines apply to the FBI's use of this information.

Ironically, when private companies wish to use and share consumer information to assess an individual's credit, decide whether to extend a job offer, or evaluate whether to issue an insurance policy, they must comply with fairly strict rules. For example, under the Fair Credit Reporting Act, private companies cannot use consumer information to deny an individual a job, credit or insurance unless that person has the opportunity to review and correct that information.

Yet the government is subject to none of those rules when it uses that same information to identify possible terrorists, even though the consequences of mistake or abuse can be very serious. The Privacy Act was supposed to subject government agencies that collect personally identifiable information to the Fair Information Practices, but the Act's protections only apply to federal "systems of records," so the government can bypass the Privacy Act simply by accessing existing private sector databases rather than collecting the information itself. Thus, although the Privacy Act requires notice to and consent from individuals when the government collects and shares information about them, gives citizens the right to see whatever information the government has about them, and holds government databases to certain accuracy standards, none of those rules applies when the government accesses commercial information without pulling that data into a government database. Currently, the government need not ensure (or even evaluate) the accuracy of the data; it need not provide individuals with the ability to review and correct the data; and there are no limits on how the government might interpret or characterize the data. Meanwhile, plans are being discussed to promote broader sharing of data with state and local authorities, and the line between domestic intelligence and foreign intelligence has blurred.

CDT recognizes that commercial information can and should play a key role in law enforcement investigations. But agencies relying on that data should have clear guidelines for its use—guidelines that both protect individual rights and ensure the information is useful for investigative purposes.

The accuracy of the information, for example, is essential both to the effectiveness of counter-terrorism efforts and to individuals to ensure they are not mistakenly

caught up in an investigation. Marketing data and other information collected for commercial purposes are often inaccurate. Rampant identity theft threatens to pollute credit reports and other commercial databases with false information. Accordingly, a way needs to be found to build data quality standards into government uses of consumer data. Another problem is security. It is important to protect against abuse by rogue agents within law enforcement agencies. There have been recurrent news accounts of police officers using access to police computers to obtain information about celebrities or to track their ex-girlfriends; agencies should establish auditing mechanisms and other safeguards to protect against that type of unauthorized access when agencies query commercial databases. Redress is a third issue: what will be the rights of an individual if adverse action is incorrectly taken on the basis of erroneous or misinterpreted commercial data?

B. Data Mining Technology

A related but even more complicated set of issues concerns so-called "data mining" or "pattern analysis" technology. This set of techniques purports to be able to find evidence of possible terrorist preparations by scanning billions of everyday transactions, potentially including a vast array of information about Americans' personal lives. This type of "pattern-based" analysis is to be distinguished from more traditional "suspect-based" searches, where a law enforcement agency has identified a suspect and is attempting to locate additional information about the suspect (or his associate) through the use of commercial databases. Pattern-based searches heighten civil liberties concerns because they require government access to everyone's information, not just that of individuals already under suspicious as a result of traditional investigative means. For that reason, our concerns about the use of private sector information (and government data originally collected for non-law enforcement or intelligence purposes) grow exponentially when the government seeks to use that information as part of a data mining program.

Congress has put a temporary hold on domestic deployment of data mining technology originating from the Pentagon's "Total Information Awareness" (recently renamed "Terrorism Information Awareness") program, and it appears likely that the hold will continue through FY2004. This is a positive step, but data mining of Americans' bank, credit, medical, commercial and other records can continue unhampered at the FBI, CIA, the Terrorist Threat Integration Center (TTIC), and the various components of the Department of Homeland Security. Yet there is a host of unanswered questions regarding this technology that should be answered before it goes forward.

These questions fall into two categories. First, is the technique likely to be effective? If not, there is no reason to pursue it, particularly when we have limited resources for counter-terrorism. No government agency has yet demonstrated that this type of technology will work, and there are serious questions about whether it will generate so much information—including false positives—that it will be impossible to investigate all of the leads. Our intelligence agencies are already overloaded with information they do not have the resources to analyze; adding to that load will serve no purpose.

Second, if data mining is shown to be effective, what should be the rules governing it? Who should approve the patterns that are the basis for scans of private databases and under what standard? What should be the rules limiting disclosure to the government of the identity of those whose data fits a pattern? When the government draws conclusions based on pattern analysis, how should those conclusions be interpreted? How should they be disseminated and when can they be acted upon?

Adapting the Privacy Act and other Fair Information Practices to government uses of commercial databases is one way to look at setting guidelines for data mining. But some of those principles seem inapplicable to the intelligence context, while others need to be further augmented. Perhaps one of the most important elements of guidelines for data mining would be rules on the interpretation and dissemination of hits and on how information generated by computerized scans can be used. Can it be used to conduct a more intensive search of someone seeking to board an airplane, to keep a person off an airplane, to deny a person access to a government building, to deny a person a job? What due process rights should be afforded when adverse actions are taken against individuals based on some pattern identified by a computer program? Can ongoing audits and evaluation mechanisms assess the effectiveness of particular applications of the technology and prevent abuse?

All of these questions must be answered before moving forward with implementation. Meanwhile, Congress should insist on a full reporting from all agencies as to their uses of commercial databases. The privacy impact assessment concept in the Defense of Privacy Act may be an excellent framework for this kind of reporting. Then Congress should limit the implementation of data mining until effectiveness

has been shown and guidelines on collection, use, disclosure and retention have been adopted following appropriate consultation and comment. It is time for Congress to create this framework, working with the intelligence agencies, privacy experts, and the industries that hold this data and build the technology to analyze it.

IV. CONCLUSION

CDT commends the Subcommittees for holding this important hearing. Enactment of the Defense of Privacy Act is an important step toward ensuring that federal agencies consider and address the privacy implications of their programs. Further steps must be taken, however, to ensure that our law enforcement and intelligence agencies operate under a set of privacy-protective polices and guidelines when they access commercial information and seek to "mine" it in search of terrorists. Such guidelines would not merely to protect individual rights; they would focus government activity and make it more effective.

Mr. CANNON. I didn't mean stop. I was really interested in what you were saying, Mr. Dempsey, but we'll give you a chance to continue in a moment.

Mr. DEMPSEY. Yes, sir.

Mr. CANNON. I just thought I'd point out here that many of the things you talked about that we've done historically were actually done under the leadership of Mr. Barr when he had this chairmanship, and I hope that I can fulfill the shoes or the mantle that he's left behind.

We'd also like to recognize the presence of—let's see, Mrs. Blackburn from Tennessee, Mr. King from Iowa, and Mr. Coble from North Carolina, and Mr. Flake from Arizona.

And with that, Ms. Murphy, we'd like to yield you 5 minutes.

STATEMENT OF LAURA W. MURPHY, DIRECTOR, AMERICAN CIVIL LIBERTIES UNION, WASHINGTON NATIONAL OFFICE

Ms. MURPHY. Thank you, Chairman Cannon, Chairman Chabot, and Ranking Member Nadler and the Members of the Subcommittee. I'm pleased to testify in favor of the Defense of Privacy Act on behalf of the ACLU, and I'm also pleased to substitute for my dear colleague Gregory T. Nojeim, who could not be here because of a family emergency.

Ours is a nationwide nonprofit organization with over 400,000 members, not 250—I have to update my bio—dedicated to protecting the principles of freedom set forth in the Constitution and in our Nation's civil rights laws. We join many Members of the Subcommittee on both sides of the aisle in nongovernmental organizations from across the political spectrum in support of this legislation.

Americans right to privacy is in peril. Individuals' personal information, including medical and financial records, is being collected on computer networks that can be linked, transferred, shared and sold, often without consent or knowledge of the person to whom the information pertains, and as Jim says, this information is increasingly being used by the Federal Government. Increasingly, this information is obtained by the Government, and because of this, legislation such as H.R. 338, the "Defense of Privacy Act," is essential to force the Government to even consider protecting the privacy of and limiting access to the information that it collects.

The legislation that you are considering today is simple, yet very powerful; modest, yet effective. It would require Federal agencies

to issue privacy impact statements with the regulations they propose. It would encourage agencies to develop a systematic means for reviewing how a particular regulation would affect individual privacy.

One need only to look at the application of this law, of this bill, had it been law when the Government introduced the Total Information Awareness program and the Computer-Assisted Passenger Profiling System. We could have used this law in the current debate that's taking place over this last session of Congress. The TSA, the agency that is advocating CAPS, wants to collect data on every individual who flies on an airplane in the U.S. To determine who is rooted in the community so that unusual behavior of less rooted individuals would help to single out terrorists. The Department of Defense wants to collect information on everyone in our country so that it can be compiled in a central database. Using algorithms they would single out aberrant behavior to help determine terrorism activities. These agencies, if they issued regulations on these programs, would be forced to consider what data it would gather on individuals and whether it could collect less data and achieve the same security outcome that it could get by collecting less data.

This legislation introduces long-accepted principles of fair information practices into the rulemaking process. It is modeled after the Regulatory Flexibility Act, and it places an important check on agencies' use and disclosure of personal information.

People care about privacy, and that's why so many people in the last year alone have joined the ACLU. Under this bill, they would have a better opportunity to be heard when their privacy is threatened.

I agree with Mr. Barr: This bill is modest because what it does not do is as important as what it does do. The bill does not create new substantive legal standards for the use and disclosure of individually identifiable personal information, information maintained by Government agencies. The Privacy Act and other Federal statutes already do that.

The bill does not give the individual power to force an agency to adopt a particular privacy policy alternative, including those that would be lease intrusive of privacy. It merely requires agencies to consider less intrusive alternatives and to explain why they selected that alternative over the others.

The bill is not overly burdensome, and it would not hinder efficient functioning of Federal agencies.

The legislation applies only to rulemaking. It does not cover other, more numerous administrative actions that fall outside the formal rulemaking process. These are things like adjudications and informal agency actions. In particular, law enforcement agencies would continue to be able to investigate crimes and track down criminals just as they do under current law. The bill includes necessary exceptions that already appear in current law.

And I think I'll conclude here. But I just would like to say that we would like to work very closely with both sides of the aisle to get this legislation into law, and I think it is very important that we had Chairman Grassley to testify over here because we don't have as many conservative privacy advocates on the Senate side as

we do on the House side. And I thank all the Members of this panel for holding a hearing today and pushing this most important legislation.

Mr. CANNON. Thank you, Ms. Murphy.

[The prepared statement of Ms. Murphy follows:]

PREPARED STATEMENT OF LAURA W. MURPHY

Chairmen Chabot and Cannon, and Ranking Members Watt and Nadler:

I am pleased to testify today on behalf of the American Civil Liberties Union in favor of the Defense of Privacy Act, H.R. 338. The ACLU is a nationwide, non-partisan organization of nearly 400,000 members dedicated to protecting the principles of liberty, freedom, and equality set forth in the Bill of Rights to the United States Constitution and in our nation's civil rights laws. For almost 80 years, the ACLU has sought to preserve and strengthen privacy in many aspects of American life.

Americans' right to privacy is in peril. Individuals' personal information, including medical and financial records, is being collected through an ever expanding number of computer networks and being stored in formats that allow the data to be linked, transferred, shared and sold, often without consent or knowledge.

The same technological advances that have brought this country enormous benefit also make people more vulnerable to unwanted snooping and accidental disclosure of personal information. The federal government's increased reliance on computerized records increases efficiency but also poses significant challenges to privacy.

H.R. 338, the "Defense of Privacy Act," would require federal agencies to issue privacy impact statements with the rules or regulations they propose. By requiring privacy impact statements, the bill would encourage agencies to develop a systematic means for reviewing how a particular regulation would affect individual privacy. In addition, such statements would put the public on notice about the choices federal agencies are making about the use and disclosure of individually identifiable information and give the public a carefully limited chance to participate in those decisions.

The Defense of Privacy Act would provide an important check and balance on federal agencies' use and disclosure of personal information inside and outside the government. The passage of this legislation would be an important step in the effort to protect privacy, particularly as the federal government relies more and more on powerful information technology.

THE HISTORY AND LESSONS OF THE "KNOW YOUR CUSTOMER" BANKING REGULATION

The history of the "Know Your Customer" ("KYC") regulations provides important background on the need for privacy issues to be considered before a regulation is adopted.

In 1998, pursuant to the Bank Secrecy Act and other federal law, each of the bank regulatory agencies published parallel "Know Your Customer" regulations to facilitate the filing of suspicious activity reports, an element of the agency's broader anti-money laundering initiative. Although most banking institutions already had adopted KYC programs voluntarily, the proposed regulation established uniform standards across the banking industry. Banks were required to identify customers and their normal and expected transactions, to determine the customer's sources of funds for transactions involving the bank, and to monitor daily transactions and identify those that appear suspicious. The impact of the regulation, however, would have been to require banks to track innocent individuals in their day to day financial transactions and collect and track an enormous amount of personal financial information through federal databases

In 1999, the Treasury Department was overwhelmed by almost 300,000 comments on the proposed "Know Your Customer" regulations because the agency failed to consider the privacy implications of tracking customers' routine banking activities and reporting personal financial information to the government before proposing the rule. As a result, the agency was forced to retreat and withdraw the proposed rule.

The KYC experience provides two clear lessons. First, Americans care about the privacy of personal information. Out of the almost 300,000 comments submitted on the proposed KYC regulations, only a small fraction were in favor the regulation. Second, federal agencies must consider privacy up front. As demonstrated by the proposed KYC regulations, because bank regulators failed to consider privacy, the proposed regulation unraveled, forcing regulators back to the drawing board and wasting federal resources.

REQUIREMENTS OF THE DEFENSE OF PRIVACY ACT

Although federal laws regulate the use and disclosure of personal information within the government, privacy continues to be an afterthought in the development of federal policy. In addition, the public has little opportunity to comment on—or even understand—the choices administrators are making about the use and disclosure of individually identifiable information.

The Defense of Privacy Act would establish basic checks and balances on federal agencies' decisions to use and disclose personal information. The legislation's "privacy impact statement" builds the principles of Fair Information Practices into the rulemaking process and would enhance individuals' control over personal information stored in government databases.

The bill would require agencies to engage in a systematic review of privacy before federal regulations are adopted and irreversible privacy violations occur. In addition, it would enhance federal agencies' public accountability for decisions about the use and disclosure of personal information.

This legislation is modeled after the Regulatory Flexibility Act ("RFA"). 5 U.S.C. § 601 seq. For over twenty years, it has required agencies to consider the needs and concerns of small business whenever they engage in rulemaking subject to the notice and comment requirements of the Administrative Procedure Act ("APA") or other federal law. This bill adopts requirements almost identical to those found in the RFA. Instead of assessing the impact on small business, however, the agency analyses would assess the impact of a regulation on individual privacy.

WHAT THE BILL WOULD DO:

Require a systematic review of privacy issues before a regulation is adopted.

Sections 2(a) and (b) would require federal agencies to issue initial and final privacy impact analyses whenever the agency is required under the APA or other federal law to publish a general notice of proposed rulemaking, including interpretative rules involving tax laws.

The "initial privacy impact analysis" would be published with the agency's proposed rulemaking and the public would have an opportunity to comment on the privacy impact statement and the underlying regulation. The contents of the impact analysis would include an assessment of the extent to which the proposed rule will impact individual privacy interests including: 1) what personally identifiable information is to be collected, and how it is to be collected, maintained and used; 2) whether and how individuals can access the personal information that pertains to them; 3) how the agency prevents the information collected for one purpose from being used for another purpose; and 4) what security safeguards are in place to prevent unauthorized disclosure of personal information. Most importantly, the agency must describe alternatives to the proposed rule which accomplish the policy objective but minimize impact on individual privacy.

A "final privacy impact analysis" would be issued with the final rule or regulation. This final privacy impact statement would include the same categories of information as the initial impact statement. In addition, the agency would have to explain the steps it has taken to minimize the "significant" privacy impact on individuals, including the factual, policy and legal reasons for selecting the alternative adopted in the final rule and why the other alternatives were rejected. The final privacy impact statement would also summarize the significant issues raised in the public comments.

Enhance public participation and agency accountability for individual privacy interests.

Section 2(d) would require the federal agency proposing a rulemaking that would have a "significant privacy impact on individuals, or a privacy impact on a substantial number of individuals" to ensure individuals have been given an opportunity to participate. Agencies could do this by taking steps such as announcing the rulemaking's potential privacy impact in publications with a national circulation, holding public hearings and conferences, and directly notifying interested individuals.

Section 2(f) would provide individuals who are "adversely affected or aggrieved" by final agency action to obtain judicial review of compliance with the procedures for final privacy impact statements.

Section 2(e) would require a periodic review of rules that have a "significant privacy impact on individuals, or a privacy impact on a substantial number of individuals" to determine whether a rule can be amended or rescinded to minimize an adverse privacy impact. Such review is required to take place within ten years of the date of enactment of the regulation. Agencies are also required to publish plans for

these reviews in the Federal Register and invite public comment on whether the rule should be rescinded or amended.

WHAT THE BILL WOULD NOT DO:

The Defense of Privacy Act would take important steps to protect privacy. Equally important, however, the legislation would not undermine government rulemaking process or inhibit important government policy goals.

First, the bill does not create new substantive legal standards for the use and disclosure of individually identifiable personal information within the federal government. The Privacy Act and other federal statutes continue to regulate the use and disclosure of personal information held by federal agencies. Sections 2(a) and (b) of the bill simply offer criteria that would be used to measure the privacy impact of any particular regulation.

Second, the bill does not give an individual the power to force an agency to adopt a particular policy alternative. The final privacy impact analysis requires agencies to articulate the available policy options and state why one alternative was selected over the others. But, the bill does not require the agency to adopt the alternative that is least intrusive on privacy.

Third, the bill is not overly burdensome and would not hinder the efficiency or functioning of federal agencies. The legislation only applies to rulemaking, not to the vast amount of administrative action that falls outside the formal rulemaking process, including adjudication, informal action, and guidance. Law enforcement agencies would continue to be able to investigate crimes and track down criminals just as they do under current law. In addition, a privacy impact analysis would only be required if a rulemaking is required in the first place. The APA includes exceptions that exempt certain agency functions from the rulemaking process altogether, including when rulemaking procedures are "impracticable, unnecessary, or contrary to the public interest." In addition, privacy impact statements could actually increase efficiency by cutting down on privacy debacles like the proposed KYC regulation. Lots of government resources were wasted on that proposed rule because there was little to no consideration of privacy in the development of the proposed regulations.

Fourth, the bill would not result in an overwhelming amount of litigation. Judicial review is limited to review of agency compliance with the procedures related to the final privacy impact statement. It does not provide individuals a right to sue over substantive decisions the agency makes in the final regulation. In 1996, the Small Business Regulatory Enforcement Fairness Act established the same judicial review provisions in the RFA as are included in this legislation. Pub.L. 104–121.

Finally, the legislation includes the same waivers available under the RFA. Privacy impact statements would not be required when emergencies make compliance "impracticable."

CONCLUSION

The ACLU strongly commends Chairman Chabot (R-OH) for introducing this important bill. We urge other Members to join them in support of a good government measure that would enhance individuals' privacy.

Mr. CANNON. I think that we have probably helped the ACLU here with the PATRIOT Act. I think that was probably the cause of the spike of——

Ms. MURPHY. It's sad, though, that things like that have to help the membership of the ACLU.

Mr. CANNON. It is, I suppose. But let me just say that it's really nice to know there are 400,000 people out there that care enough to sign up and pay their dues. So we appreciate that.

I'll yield to myself 5 minutes, and then we'll—oh. I think we want to acknowledge the presence of our Ranking Member on the Commercial and Administrative Law Subcommittee Mr. Watt.

Mr. WATT. Good morning.

Mr. CANNON. May I just ask, Ms. Murphy, you know, you talked about CAPS. My understanding of CAPS is that it's really a private database that the Government is adopting. Is that true?

Ms. MURPHY. Well, it is a database, but I don't know how you can call it private when the Government adopts it.

Mr. CANNON. Right. But it comes from—it was created by the—by one or more of the airlines and used, as I understand, in a primitive form to identify many of the terrorists on 9/11 and has now become more central to the Government activity.

Ms. MURPHY. Right. Well, the genesis of CAPS has come from the airline industry—the fact that the Government is now going to be responsible for administering this program, in my view, makes it something completely within the purview of the Government, and the troublesome part of CAPS is that they did not issue regulations in advance of the program. So this bill would not necessarily capture CAPS-related regulations, and we need to look at ways to find—to force and compel the agencies to issue regulations and come to Congress before they institute such invasive programs.

Mr. CANNON. Thank you.

One of the things I'm concerned about is there are a lot of private databases out there. There are databases, huge databases, that are being manipulated by private companies. Much of their information comes from public records, but it seems to me that this is a critical interface between what is private and what people can do with private databases, which I think is quite scary also, and the governmental interface.

Let me ask you a question that I would like each of you to respond to. You know, I was concerned, and when I watched and I forced all my kids and all my staff to watch Enemy of the State, because that's an interesting movie, what you have there—a couple of things that are really intriguing as it relates here. One of them, obviously the movie is about an innocent citizen who is the victim of a bent bureaucrat with lots of power. And that's scary to everyone. But just as scary is the fact that you have a—well, I get—it's actually a nice thing. You have a Congressman who's represented as being a man of principle. Since he couldn't be bought or bribed or black-mailed, he was killed. I suppose—that may be a more rare circumstance than reality. The nice thing is that you actually had someone who was portrayed as being honest and having integrity. The unfortunate thing is that you have to get rid of him.

But I worry there aren't a lot of us that would be in that circumstance. But there are a lot of us who are mortal and who can be pushed around by data. And so there are two sorts of things. I'm really trying to grapple with what this transition in our society where we have so much computing power, so much ability to manipulate, so much ability to sort in comparison to the available data that it seems to me that we have a couple of problems, and I'd like your insight on those problems, what other problems we have to go along with that.

In the first place, you have the problem of public officials who are subject to extortion because of facts that can be observed through these databases, and, therefore, you get a distorted decision-making process. And then the second concern that I have is, you know, if someone wants an outcome from Congress, like the person did in Enemy of the State, he can get it by extortion. But on the other hand, I worry about the lower agent who has a potential son-in-law that he doesn't like and he wants to dissuade him

from marrying his daughter, and therefore goes in the database and finds information.

It seems to me that when you get into that position, you're not much different from some of the States in the world where they use thuggery or bribery or some other form of persuasion other than law to regulate society, and it occurs to me that those two things seem to be critical issues that we ought to be dealing with, that they go well beyond this issue. But I'm wondering, as you've looked at the big questions, are those the big questions, or are there other things out there that we need to be concerned about?

We can start with Mr. Barr.

Mr. BARR. You've raised some very important and fundamentally critical issues, Mr. Chairman, as you always do. And I think those are certainly concerns. A generation ago or so when I was in college, back in the 1960's, we had some scandals back then with regard to the Government, certain Government agencies collecting evidence and compiling dossiers on certain citizens in the civil rights movement and the student movement and the antiwar movement, and that was bad enough. Think what the problem would have been had they had today's technology in those times.

You are right. The availability of the technology, the extent to which technology can be used to collect, analyze, sort, disseminate vast amounts of data, undreamed of just a few years ago, really puts us in an entirely different arena than we were a generation ago, and that influences why we are here today, and it influences what Government can do. The Department of Defense coming forward and saying, you know, hey, it's okay, guys, we're only going to limit the collection of information that goes into TIA to that information which Government can accumulate lawfully, doesn't make me feel any better whatsoever.

The problem here is, and the question here is, do we want Government to be doing this in the first place regardless of where it gets the data. Whether it gets it from a private database as a way to avoid the strictures of the Privacy Act or FOIA, for example, or whether it gets it from somewhere else, the fundamental question is do we want Government gathering data, analyzing it and compiling electronic dossiers on law-abiding citizens with no reasonable suspicion that they have done anything wrong? That is why this debate is so very, very important and why the answer to your question is yes, those are very, very real concerns today, and if we don't address them today, we'll not have an opportunity to in a few years. It will be a fait accompli.

Mr. DEMPSEY. Mr. Chairman, I think you have put your finger on it exactly in terms of asking what is the next set of issues that we need to worry about. I think H.R. 338 should be enacted, address the regulatory process and the collection in the regulatory process. Get that done and in place, but at the same time, begin to move on to the kinds of questions that you're now raising. And one of those is this blurring of the line between commercial databases and Government databases and the increasing reliance of the Government on the commercial data.

The Government—the day of the centralized database of the Big Brother Government computer is beyond us.

Technology has moved in a different direction. The technology has become decentralized. The technology has become privatized. And now the Government no longer has to collect the information into a central database. The Government can reach out to these commercial databases. And currently, those are beyond the reach of the Privacy Act. They would be beyond the reach of H.R. 338 as it currently exists.

I think the first step is to find out what commercial databases is the Government purchasing or using or subscribing to, what is the accuracy of that data? How is it being used? If you are in the database and you are in there wrongly, how can you A, find out, B, correct it? What is that being used for? If it's brought into the criminal justice system, you get the full panoply of constitutional rights in a trial, but if it's used in an employment context or some kind of screening context or voting or if it's used in any of these noncriminal justice contexts, it's not clear to me what the limitations are.

As Mr. Barr correctly pointed out, the privacy laws just are not attuned to this current environment, and this is where I urge this Committee—these Committees to direct their attention. Let's get H.R. 338 out of the way. Hopefully, we can find a Senate cosponsor and move it forward. It's earlier in the Congress this year. Let's get this enacted, but begin to use this as the way to think about the kinds of issues you're raising.

Mr. CANNON. Thank you, Mr. Dempsey. I am well over my time.

Mr. Nadler, would you like to—the Chair yields 5 minutes to Mr. Nadler, the gentleman from New York.

Mr. NADLER. Thank you, Mr. Chairman.

Mr. Dempsey, could you elaborate a little bit on the issue of the misuse of information once it's obtained, for example, inappropriate sharing and identity theft, and how we might deal with that?

Mr. DEMPSEY. Well, as we all know, identity theft is one of the fastest growing—probably the fastest growing crime in the United States. If you are the victim of it, it can ruin your life as you try to recover from it, not only the initial monetary loss, but then in the process of trying to clean up your records.

It is also interesting to think that the process of identity theft is continually polluting these databases and introducing false data into them. The State of California alone has a terrible problem through its Department of Motor Vehicles issuing driver's licenses which have biometrics in them. They have the ID. I think they have a fingerprint on them, and they're issuing them to the wrong people. So you are walking around with a Government-issued ID that's not reflecting your real background and your real identity. And then you begin creating a whole new database of information, again, perhaps under somebody else's name.

Part of the basis for this is the Social Security number. The Social Security number clearly was designed to administer the Social Security system to collect and account for the payments. It was originally supposed to be used only for that purpose. Our society, our Government has violated one of the fundamental privacy principles, which is that the information collected for one purpose or a record collected for one purpose should not be used for another pur-

pose. We now see that number everywhere, and it has become the key to identity theft.

I think, perhaps, we can get that cat actually back in the bag as we develop new information systems and new information collection and begin using identifiers other than the Social Security number and sticking to the principle that you should have different identifiers for different systems if feasible. But identity theft is at the core. I think both of the questions of security and of some of the other issues, that H.R. 338 would force Government agencies to pay more attention to.

Mr. NADLER. Thank you.

Ms. Murphy, Senator Grassley commented on the case for effective checks in the executive branch, especially in this area. The bill before us provides for judicial review. Do you have any concerns about the Administration's position on judicial oversight of national security agencies?

Ms. MURPHY. Yes. We have substantial concerns, because I think one of the problems with the PATRIOT Act is it wrote out significant judicial review in areas that have to do with personal privacy. So when it comes to business records, academic records, library records, the standard for judicial review is not strong enough so that the Government is forced to justify a need nor that information. And when you look at section 215 of the PATRIOT Act——

Mr. NADLER. You are saying it is not strong enough to make the Government justify——

Ms. MURPHY. That's right. And when you look at section 215 of the PATRIOT Act in particular, the Government only needs to assert to a court that the information its seeking is relevant to a terrorism investigation. So increasingly, through antiterrorism laws that are morphing into crime fighting laws, as we have seen with the use of the PATRIOT Act and whether it is sneak and peek warrants in other areas of the laws, increasingly the ability of the Government to seize information without our knowledge is—the need for that power is being claimed by the Government in order to fight terrorism when, in fact, we know that what happens to these laws and other laws that allow the Government to get our data, mission creep occurs and what's sought for one purpose, is used for another purpose. And that's a constant problem in the context of privacy.

Mr. NADLER. And this, of course, leads right into the question that Mr. Dempsey talked about information being collected for one purpose and being used for another purpose. Can you comment Mr. Dempsey or perhaps Mr. Barr, either one, on how the PATRIOT Act leads to or should we put more restrictions on it with respect to the use and the promotion of information being collected for one purpose and being used for another?

Mr. DEMPSEY. Well, the PATRIOT Act appropriately addressed the question of the sharing of information between the law enforcement and the intelligence communities and eliminated some of the legal barriers to the sharing of that information from the law enforcement side to the intelligence side. There never were any legal barriers preventing intelligence agencies from sharing their information with law enforcement. The fact they didn't do that well had nothing to do with privacy legislation or statutory burden. That was purely a question of turf and institutional issues, which I still

don't think are addressed by the way. But the PATRIOT Act said that information collected for law enforcement purposes under the Grand Jury Authority, under the Title III Wiretap Authority, could henceforth be shared with the intelligence agencies.

Now, when Congress created the Department of Homeland Security and gave it the intelligence, fusion and analysis function of taking all of this information from the law enforcement side and from the intelligence side and putting it together, trying to connect the dots, Congress set up an Officer for Civil Rights for the Department of Homeland Security and a Privacy Officer and gave those officials explicit authority to address the privacy concerns.

Now, what has happened? The President has taken that intelligence fusion and analysis function away from the Department of Homeland Security and given it to an agency, the so-called TTIC under the CIA, where there is no Privacy Officer that anybody knows of, where there is no Civil Rights or Civil Liberties Officer, and where there is not the congressional oversight. Actually, the full Judiciary Committee, along with the full Homeland Security Committee, are holding a hearing this afternoon on this very issue where this will be raised. But that's an example of where I think Congress to some extent in the Homeland Security Act may be recognizing that the PATRIOT Act had gone overboard in some respects and didn't have the adequate checks and balances. I think Congress was trying to create some oversight in the Homeland Security Department, and now we are seeing all of that analysis and sharing and accumulation of information occurring outside of that oversight process.

Mr. NADLER. Can I ask one more question with the indulgence of the Chair?

Mr. CANNON. Without objection.

Mr. NADLER. You said that the PATRIOT Act—that was never a bar—no aspersions—there was never a bar for sharing of information gathered by intelligence agencies for law enforcement purposes and that what the PATRIOT Act did was to enable the sharing of information gathered for law enforcement purposes for intelligence. I thought it was the other way around. And I would think that since we established in the FISA act of 1979 I think it was, a lower bar for gathering—for invading privacy and gathering information, for suspected foreign intelligence agents, that under the 4th amendment, in other words, you don't need the same evidence and the same probable cause to get a search warrant and so forth for foreign intelligence, that since you now are invading peoples' privacy if you are suspected of being a foreign intelligence agent in a way you wouldn't do if you suspected them of being thieves or murderers, that the point is, if they are not foreign intelligence agents, you have to protect against that information coming into the domestic criminal side, because otherwise you are undermining the 4th amendment, and it's not the other side that is the other problem because you have a higher standard before you can collect the information on the other side.

Mr. DEMPSEY. Congressman, you are talking about what is called the Primary Purpose Test. Under the Primary Purpose Test, which was used in the Foreign Intelligence Surveillance Act, the primary purpose of the surveillance had to be the collection of foreign intel-

ligence or counterterrorism information because of the lower standard. That was the purpose. But once that information was collected——

Mr. NADLER. If you met that purpose.

Mr. DEMPSEY. If you met that purpose, under FISA from 1978, it was always permissible to share that information with the law enforcement authorities, and there were 50 or 60 or 70 cases where that was done, obviously espionage cases which start out as counterintelligence cases turn into criminal espionage prosecutions, that could always occur.

The problem that I saw, and others saw, with the PATRIOT Act was starting out with the purpose, the going in for the purpose of collecting criminal evidence under that lower standard. Now, the Justice Department and the FBI really got their knickers in a twist with the FISA court misinterpreting that whole——

Mr. NADLER. They misinterpreted or the court misinterpreted?

Mr. DEMPSEY. It was unfortunately done in secret, even the interpretations of law. They all were just flat out misinterpreting that legislation in a way that did not really even protect privacy, and they had this almost perverted interpretation of that law saying that they had to create this complicated law and went in swearing, the FBI and Justice Department, that there was no criminal interest in people where there clearly was a criminal interest. The whole thing got completely perverted in a way that did no good for privacy and no good for national security.

I am not sure that the solution Congress picked was the right solution. I think that merits revisiting. But it's a classic case of where you take the interpretation of law and put it into a secret box. It's all ex parte. It's only the Government talking to the Government, and it did not well serve either privacy or national security.

Mr. NADLER. Thank you, and I thank the Chair for his indulgence.

Mr. CANNON. This is really quite an interesting hearing. I feel badly having gone way beyond my time. Maybe we can go to a second round if there are more questions.

Mr. Chabot?

Mr. CHABOT. Obviously, I think we would all agree we want to do whatever we can to make sure that our country is protected from terrorism and that we're safe as we possibly can be. But as the Government discussed this program, such as the Defense Department's Total Information Awareness Program as you had mentioned, Ms. Murphy, and the Transportation Security Administration's Computer-Assisted Passenger Prescreening System, I think what you addressed as well, does it seem that either the Defense Department or the TSA took sufficient time, looked closely enough at privacy implications on law-abiding citizens, and how do you think considering personal privacy rights during the regulatory process could have enhanced or improved these particular regulations?

And I'd ask each of the members if they would like to address that. Mr. Barr, I go to you first.

Mr. BARR. Of course, Mr. Chairman, a fundamental problem is no matter what mechanism you have in place, if you don't have

people who care about it and whose mission it is to abide by the law, the system is not going to work. One of the reasons that I suspect, for example, that we see more and more Federal agency use of outside databases, that is private databases, is for the very reason that Mr. Dempsey indicated, and Mr. Nadler expressed concern about, in his opening statement, and that is to avoid the strictures of the Privacy Act or in some cases FOIA. If, in fact, the agency can tell an aggrieved person, who believes they are aggrieved, they don't know it, perhaps, but they believe they are an aggrieved party because the Government has misinformation on them or is misusing information on them, they can avoid having to answer any questions or disclose the information by saying it is not our information, it is not a Government file. That is an increasing problem. And it's one reason why I do think that an additional matter that the Congress needs to look into is the Privacy Act itself and Freedom of Information Act. These laws were put together for very laudable purposes a generation ago, but now the technology that's now available both to private industry and to the Government is light-years ahead of where it was when these laws were crafted. So I think that's a very real concern. Whether or not some of the problems that we're now seeing would have come to light with regard to the Total Information Awareness or whatever they are calling TIA nowadays or CAPPS II, could have been avoided by a more timely and a more public, you know, exposure to this and discussion of this, I think clearly, yes. But the problem is that the development of TIA is not something that Congress mandated in the first place. It wasn't that the Defense Department said—had this forced upon it. It was an idea that they took some general language, and I think it was in the Department of Homeland Security Bill, and said, hey, this means we've been given this general charge to try to come up with ways to better identify terrorists, and they take that ball and ran with it in all sorts of different directions.

The one point that Senator Grassley made before he had to leave is a very, very important one and that is no substitute for true oversight, not just occasional oversight, not just superficial oversight but to ask some fundamental questions about some of these programs that are being developed because they do not reflect congressional intent.

Mr. CHABOT. Let me just mention something that you mentioned, Bob, about the oversight. If we're successful in passing this legislation, and I think, ultimately, we will be, I think we have to be very vigilant that it doesn't become "check this form" or this is a "thing done by the agency" and no one takes it seriously. So I think we have to have considerable oversight to make sure that every department goes through every regulation and rule to ensure that Americans' privacy rights are protected.

Mr. Dempsey?

Mr. DEMPSEY. Mr. Chairman, that certainly is an excellent point you just made. In terms of the CAPPS II Program, the Air Passengers Screening Program of the Transportation Security Administration, I will say that that agency is now seriously considering the privacy issues. They have now a Statutory Privacy Officer, Nuala O'Connor Kelly,

Who I think was an excellent choice for that job and is really trying to bring attention to the issues.

The Agency, before she came on board, issued a Privacy Act Notice which was completely unintelligible. You couldn't even tell what they were talking about and they were basically saying, well, we can do anything and collect anything and keep it for as long as we want. They are now in the process of drafting a new Privacy Act Notice. They are also in the process of doing a Privacy Impact Assessment, because, as I said, the Homeland Security Act does provide for Privacy impact assessments, unlike other Government agencies. I'm afraid that the—I'm still not sure how that's going to come out. I'm still worried about mission creep, terribly worried that some in the Agency are going to try to take an air passenger screening system and turn it into a general law enforcement system, which I think would be a disaster for both privacy and air safety.

In terms of TIA, I spent, personally, a fair amount of time now with Dr. Popth, the Deputy Head of that and the person in charge of TIA. They are trying to understand the privacy issues. They had to be brought to it by Congress, by the Grassley amendment and forced to issue a report. The report still doesn't come close to answering the questions, as Mr. Barr alluded to. They say in the report, we will only use in TIA, the information to which we are lawfully entitled. Well, we've gone through the various privacy laws and shown that again and again in those laws, there are major loopholes for national security or for intelligence, et cetera. Now obviously, we have a serious terrorist threat that we face, and absolutely we need to use information and information technology as one of our strongest weapons in that fight. But to say that there will be a blanket exception, I think, undercuts both the security goals as well as the privacy values. And we need to build those checks and balances back in. I think on the TIA, we're not close to there yet. Particularly, when we think about how that will be deployed outside the Department of Defense, and how, perhaps even not under TIA, agencies are developing data-mining capabilities already, which needs to be looked at.

Mr. CANNON. Thank you, Mr. Dempsey.

If I might just point out, you have touched on the whole array of issues that we need to be concerned about. I want to thank Mr. Barr for his foresight when he was Chairman of the Commercial and Administrative Law Committee in identifying these privacy issues, establishing an oversight or an approach to them. And on the Judiciary Committee, we need to figure out where we are going to do this and continue to do it so that we have an oversight function that is effective. I just don't think we have it anywhere else in Congress. So I thank you very much for that.

Mr. Scott, would you like to ask questions?

Mr. SCOTT. Sure.

Mr. CANNON. The gentleman is yielded 5 minutes.

Mr. SCOTT. Thank you, Mr. Chairman, and I thank you for calling the hearing. I would like to thank all of our witnesses. Mr. Barr, many others, worked on the PATRIOT Act, and I think made significant improvements in that Act as to some real constitutional problems and appreciated working with him on that and other bills

where privacy was an issue. Mr. Dempsey and Ms. Murphy have been outspoken critics of many things that this Committee has done, and I think we have benefited from that criticism.

Mr. Dempsey, I share the same concerns as the gentleman from New York pointed out with getting information under the—under FISA, where there is virtually no limit to what you can get. Bona fide curiosity is about the only standard you need to get information under FISA. And when you can start using that in criminal investigations, I think you have gotten into real problems, particularly when all these people are working together, FBI agents and TIA agents working on the same task force, you have the incentive for one to say, you can get it and don't have to worry about probable cause, and if you find anything, let us know, offers real problems.

So I just want to indicate that I share the same concerns that he did. One of the questions on the legislation, I think, we see what the problem is. The question is how this bill would actually help. What information would no longer be available if this bill had been in force?

Mr. DEMPSEY. I think that we would have seen a more careful design of information collection. I think in the Committee report last year on this legislation, it pointed out, for example, the kind of information that is being collected under some of the Federal health care systems where just a huge amount of information is being collected, stored under the Social Security number, and I think that if this bill had been in place, the question would have been forced, do you really need to collect all of this information? Do you need to store it under a Social Security number, where it's most vulnerable to theft and misuse? Do you need to keep it forever, or shouldn't you establish some limits on how long it can be kept?

I think if you're looking at the Veterans' Administration computer systems, if you are looking at the Health and Human Services new-hires database, I think there are a host of regulatory databases that were created over the past five or 10 years which never got the kind of scrutiny. Congress may have put—as Mr. Barr suggested—may have put one sentence into legislation, but then the Agency uses as the justification for a huge data collection effort. And the purpose of H.R. 338 is to say, sort of, stop, look and listen. Pause before you go into this data collection. Solicit comments. Listen to them. Take them into account. Then the Agency can go ahead under this legislation with the data collection.

This is not telling the Government to stop doing anything. If the need is there, if the justification is there, H.R. 338 allows it to go forward. But it focuses the attention of the Agency up front in the design phase. So that they can build in audit trails, for example, to protect against abuse. Far easier to do that when you're building the system than after the fact.

Mr. SCOTT. Before my time expires, as you've indicated, does nothing check the power of a bureaucrat to get information and misusing it? Would this bill create any hardship on an agency? Is there any compliance problem with an agency complying with this?

Mr. DEMPSEY. Well, I think that they are subject to judicial oversight on this. But the CBO found last year that the legislation would not impose any significant cost on the agencies.

Mr. SCOTT. Have any crimes been discovered using all of this information that's floating around, all of this private information? Has invasion of privacy done any good?

Mr. DEMPSEY. Well, in individual investigations, this information can be very useful. When you're dealing with the question of data mining, I think there's no evidence that it's useful yet. It may be there.

Mr. Chairman, if I could just point out one example, the FINCIN, the Financial Crimes Information Network, which collects, by regulation, millions and millions of reports on banking transactions, supposedly to spot money laundering. I think reviews of that system have found that it has had very, very little, if any utility in spotting money laundering, just based upon the flows of money transactions. And yet, that continues to suck in more and more of these currency transaction reports year after year after year. I think that's an example of where this attempt to scan large databases does not produce the kinds of results. The focused, particularized suspicion of the 4th amendment does produce results, and I think that's where we need to focus.

Mr. CANNON. Thank you, Mr. Dempsey.

I think we have two more people who would like to ask some questions, and there's a vote that is coming up. And so if we keep fairly short on the answers.

Go to Mr. Coble and Mr. Watt. Mr. Coble you are recognized.

Mr. COBLE. Mr. Chairman, thank you for calling the hearing, and thank you all for being with us.

Most Americans guard their privacy very jealously, as do I. And until these murderers came calling on 9/11, many Americans and probably most Americans, regarded domestic terrorism sort of indifferently. You know, it will never happen here. I don't mean that they're uncaring about, but it will never come to our shores. Well, it came to our shores. And those who regard our privacy jealously—I don't mean that we need to compromise our privacy, but we need to be a little more flexible than we were.

Good to have you back on the Hill, Mr. Barr. How do you respond, folks, to those who say that society's interest in protecting privacy must take second place to the prevention of terrorism? Must the former inevitably fall victim to the latter, A? And B, some of the Government's most aggressive surveillance technologies, I am told, are described as being intended for overseas use. What safeguards are in place to ensure that they are not deployed domestically?

And let me start with you, Mr. Barr.

Mr. BARR. As always, Colonel, you have put your finger on two extremely important issues. The answer to the last one is, there's nothing in place. And this was a paradigm in a recent discussion played out in the newspapers with regard to something called CTS, combat zones at sea, and this is a program again being developed at DARPA, supposedly, for use in urban environments overseas by our military to marry up an array of surveillance cameras with digitized computer and facial recognition to track cars and people

over time and record and store all of that data from those cameras. As soon as word got out on this, then there have been and this is reported in the paper, police chiefs and law enforcement officials across America they're saying this would be a good tool to use in urban environment for law enforcement purposes in this country.

This is the problem—one of the problems with getting the Defense Department involved in data collection and developing techniques to gather, manipulate, store and use and possibly abuse data on citizens. There's no checks or balances on it, and that's something that Congress really needs to look at in the context of all of these different programs. And I'll leave it to perhaps, Mr. Dempsey, and I have already forgotten——

Mr. COBLE. First question.

Ms. MURPHY. I think the question is a valid one because we are asking the public to give up its privacy protections in the name of assuring national security. And I think the question we have to answer is what went wrong with the terrorism attacks that we have experienced in the United States? And I think Members of Congress should be in a position to fix the things that went wrong, rather than giving the agencies cart blanche to gather information on people who are not convicted of any criminal activity or not suspected of any criminal activity, rather than allowing those agencies to collect that data like TIA would or like CAPPS would. I think the Congress must insist that it fix the problems that will provide real solutions to our national security. And it's interesting, the ACLU is polled on these questions on about whether or not there should be these trade-offs.

And increasingly, the further out we get from 9/11, the more citizens are less willing to give up their privacy. And conservatives and focus groups, in particular, have been angered by what they see in terms of encroachments on their privacy, and they think about what would happen if Attorney General Hillary Clinton had these powers, and who would she investigate, and then people begin to step back and say look, we need to have a standard for protecting our privacy and not react in the haste of the moment. And I think most American people are reasonable. But if you asked them a month after September 11, they'll say I don't have anything to hide. Take my private information. But I think people are being much more reasonable and are questioning and challenging the Government more from all sides of the political spectrum.

Mr. COBLE. Mr. Chairman, in the interest of time, I yield back.

Mr. CANNON. I thank the gentleman. And Mr. Watt, you are recognized for 5 minutes or as much time as you may consume before we have to leave to catch this vote.

Mr. WATT. I thank the gentleman for yielding time.

And let me do two or three things. First of all, I want to join my colleague from North Carolina in welcoming our former colleague back, we missed you. We especially miss you in areas like this where individual liberties are at risk, because we need and needed that balance from both sides emphasizing these issues, and I haven't heard that as aggressively since you have been gone.

Second, thanks to the Chairman for calling the hearing. It's an absolutely necessary and important hearing.

Third, I said in a press conference when the bill was introduced originally, a couple of years ago, whenever it was, that I supported the bill. I still support it. I think it's not revolutionary. And we need to get some control over this area.

Fourth, I'm not sure that I am as optimistic as Mr. Chabot is about the prospect for moving this bill and getting it passed and signed into law. I'm a little more cynical, I think, in my views about this, because I've seen the agencies—the bureaucrats, the bureaucracy that would be potentially impacted by a bill such as this work behind the scenes, underground, undercover to sabotage the passage of a bill such as this. I don't know why it didn't move in the last term of Congress. Perhaps it was the lateness of moving it, but this bill should have moved. I've seen those agencies take the PATRIOT Act and turn it from something that was a strongly bipartisan bill in the Judiciary Committee, that we thought had the support of the Administration, to a bill on the floor that many of us could not support because the bill got rewritten between the Judiciary Committee and the floor of the House by people, most of whom weren't even lawyers and didn't understand the privacy or personal liberties consequences of what was being done.

Mr. CHABOT. Would the gentleman yield? It did pass in the House. It was in the Senate.

Mr. WATT. I know it did pass in the House, didn't pass in the Senate. I'm aware of that. Finally, I'll ask a question now that I have gotten all those things off my chest. I'm wondering if anybody can distinguish for me what the difference is between the Defense Department's Total Information Awareness Program, which is what the original name was, and the Defense Department's Terrorism Information Awareness Program? Is there substantively, in your experience, any difference between what they're doing just by changing the name from one thing to another?

Mr. BARR. Unfortunately, I don't think so, Mr. Watt. It's a trick that we've seen over and over again. You change the name of something and hope that attention will thereby be deflected at the same time. It's the same program, only by a different name.

Mr. DEMPSEY. I agree with Mr. Barr, there is no difference.

Mr. WATT. So we should be concerned?

Ms. MURPHY. I agree, too. And the fact that they have changed their Website several times and changed their name once, is an indication that they are sensitive to public criticism about their mission. So I would suggest that even though it is now called Terrorism Information Awareness, it still is vulnerable to congressional oversight and public criticism as it started out to be.

Mr. WATT. I'll say one final word. I think it's important for us to continue our vigilance in this area without bringing you all back after the votes because this Committee, the only way we can data mine into what they're data mining into is by doing effective oversight, and we need to get into all of these sources and programs and figure out what our Government is doing and in some cases what private enterprise is doing. And I strongly support that and I yield back.

Mr. CANNON. I thank the Ranking Member—and let me just point out what he calls cynicism, I view as duty. There is a duty in this body to be cynical of what the executive branch does wheth-

er they are of the same or different party. And we intend to continue this.

I want to thank our panelists—we are very short on time. You are welcome to leave here. I will just wrap here and state that I really appreciate your comments. I wish we had more time. I think it is best for you that we end this now because you would have to wait for awhile. But a number of things you said have suggested ideas for new hearings. I hope you'll work with staff and help us flesh some of those ideas out.

Along with Mr. Watt, I feel—Mr. Chabot, I feel a keen urgency about exploring these issues, about using legislation and oversight to contain the administrative and executive functions that are moving forward at a very rapid rate. So I thank you for your time and this hearing is now adjourned.

[Whereupon, at 11:47 a.m., the Subcommittee was adjourned.]